

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- 250

Date: August 21, 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. 2 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	As Addendum No. 1 of 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: 19 August 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: 26 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: 19 August 2025 Time: 12.30 hours Bangladesh Standard Time (BST= GMT + 6:00 hours).	The Proposal opening shall take place at: Address: Youth Tower (Level 5), 822/2, Rokeya Sarani, Dhaka-1216, Bangladesh Date: 26 August 2025 Time: 12.30 hours Bangladesh Standard Time (BST= GMT + 6:00 hours).



Sl. No.	RFP Reference	As Addendum No. 1 of RFP	As Amended
3.	Section: 3.7 Detailed Technical Specifications and Requirements, 3.7.8 Ticketing, IT Service, IT Asset & NMS System SL: 141-213 Page:182	Title changed as: NMS Module A	NMS Module
4.	3.7 Detailed Technical Specifications and Requirements	Serial Number Changed as: 3.7.31 SOC Trainings (With Certification Exams) 3.7.32 SOC Trainings (With Certification Exams, On-Site Global Training Partner Premises) (Free of Cost) 3.7.33 Installation & Implementation of NSOC System 3.7.34 Project Management Oversight (Non-Priced) for NSOC System Implementation 3.7.35 Service Level Agreement (SLA) 3.7.35.1 Operational and Maintenance Personnel during SLA	3.7.29 SOC Trainings (With Certification Exams) 3.7.30 SOC Trainings (With Certification Exams, On-Site Global Training Partner Premises) (Free of Cost) 3.7.31 Installation & Implementation of NSOC System 3.7.32 Project Management Oversight (Non-Priced) for NSOC System Implementation 3.7.33 Service Level Agreement (SLA) 3.7.33.1 Operational and Maintenance Personnel during SLA
5.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.28 Malware Analysis Sandbox (On-premise) "6 Performance Requirements"	The system should be capable of analyzing files of size minimum 300 MB and more	The system should be capable of analyzing files of any size upto 300 MB at least.



Sl. No. 4.

Section VII – Purchaser's Requirements

3.7 Detailed Technical Specifications and Requirements,

3.7.1 Security Information and Event Management (SIEM)

Page: 152

As Addendum No. 1 of RFP: for SIEM Probe/Sensor

As Addendum: Following Requirements Removed/Dropped after SIEM SL16 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</p>



Sl.	Feature	Requirement of Procuring Entity
		<p>external information sources.</p> <p>The solution should have capabilities to identify historical information about all endpoints (including unmanaged and IOT, if 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>

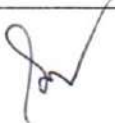
[Handwritten signature]



Sl.	Feature	Requirement of Procuring Entity
		<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> <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>



Sl.	Feature	Requirement of Procuring Entity
		<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> <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</p>




Sl.	Feature	Requirement of Procuring Entity
		<p>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> <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</p>



A handwritten signature in black ink, located at the bottom right of the page.

Sl.	Feature	Requirement of Procuring Entity
		<p>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> <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>

[Handwritten signature]



Sl.	Feature	Requirement of Procuring Entity
		<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. • 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



A handwritten signature in black ink, appearing to be "J. Am".

Sl.	Feature	Requirement of Procuring Entity
		<ul style="list-style-type: none"> • 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> <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. 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>



Sl.	Feature	Requirement of Procuring Entity
		<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> <p>The solution should be able to list all the activities of a device,with-in the time range of 60 seconds of a particular suspicious activity without writing any complicated quires.</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	<p>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</p>



Sl.	Feature	Requirement of Procuring Entity
		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. 5

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 Addendum No. 1 of RFP: SL: 215-233 NMS Module B

As Amended: Following Requirements Removed/Dropped 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



Sl.	Feature	Requirement of Procuring Entity
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
226	Alerts and Notifications	<ul style="list-style-type: none"> - 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



A handwritten signature in black ink, consisting of stylized, cursive letters.

Sl. No. 6

Section VII – Purchaser's Requirements

3.7 Detailed Technical Specifications and Requirements

Page: 185

As Addendum No. 1 of RFP: SL. 3.7.29 for VAPT Tools

As Amended: Following Requirements Removed/Removed 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
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
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 HighImpedance 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

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 12 MP, f/2.2, 32mm (standard) • Must support 4K@24/30/60fps, 1080p@30/60/120/240fps, 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



[Handwritten signature]

Sl. No. 7

Section VII – Purchaser’s Requirements

3.7 Detailed Technical Specifications and Requirements

As Addendum No. 1 of RFP: SL. 3.7.30 for Digital Forensic Tools

As Amended: Following Requirements Removed/Dropped 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.



Sl.	Feature	Requirement of Procuring Entity
		<ul style="list-style-type: none"> • 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. • 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 haveList of passwords supported by the Known Passwords attack • The Solutions Should haveLUKS2 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



[Handwritten signature]

Sl.	Feature	Requirement of Procuring Entity
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,
		<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.	DetegoAnalyse Forensic.	Renewal of license for DetegoAnalyse 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

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



Sl. No. 8

Section VII-Purchasers' requirements

Page:234-237

As Addendum No. 1 of 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



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
	Workstation (Qty. 15)		3.7.16	ICT	W6	W8	W10	No



				Tower				
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
27	External Attache Surface Monitoring		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



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
7	VPN Firewall for CII Integration (Qty. 02)		3.7.7	ICT Tower	W6	W8	W10	No
8	Ticketing, IT Service, IT		3.7.8	ICT Tower	W12	W16	W18	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
	Asset & NMS System							
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
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"		3.7.22	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
	with HDMI Matrix and Accessories)							
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
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



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
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




Sl. No. 9

Section VII-Purchasers' requirements

Page:241-244

As Addendum No. 1 of 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
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



Component No.	Component	Relevant Technical Specifications No.	Additional Site Information (e.g., building, floor, department, etc.)	Quantity
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
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



Component No.	Component	Relevant Technical Specifications No.	Additional Site Information (e.g., building, floor, department, etc.)	Quantity
31	SOC Trainings (With Certification Exams)	3.7.31	ICT Tower	Lot
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

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




Component No.	Component	Relevant Technical Specifications No.	Additional Site Information (e.g., building, floor, department, etc.)	Quantity
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
16	Workstation	3.7.16	ICT Tower	15 Unit



Component No.	Component	Relevant Technical Specifications No.	Additional Site Information (e.g., building, floor, department, etc.)	Quantity
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	SOC Trainings (With Certification Exams)	3.7.29	ICT Tower	Lot



Component No.	Component	Relevant Technical Specifications No.	Additional Site Information (e.g., building, floor, department, etc.)	Quantity
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
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

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

Enhancing Digital Government and Economy (EDGE) Project

Bangladesh Computer Council (BCC), ICT Division.

