ELCOT Adding Value through IT	**Electronics Corporation of Tamil Nadu Limited**
Tender	**Selection of System Integrator for Supply, Design, Development, Implementation and Maintenance of CCTNS 2.0** **Tender Ref.** ELCOT/PROC/OT/33384/CCTNS 2.0 (SCRB)/ 2020-21
	Corrigendum No. 1 to the Tender Document

CORRIGENDUM TO THE TENDER DOCUMENT

The following Corrigendum to the Tender Document is hereby issued:-

S.No	Title of the Clause	Existing Clause	To be read as
1	Volume 1 - Page No. 45- Clause No. 5.3 Sample Submission;	i. For each hardware item quoted in the RFP, the samples should be submitted to ELCOT indicating the make, model number and brochures / specification of the items for testing by ELCOT as per Annexure 8.2 (Sample Submission Form) of this RFP. ii. The pre – qualified bidders have to submit the samples within 7 days from the date of intimation from ELCOT unless any specific time given by ELCOT in writing.	i. For each hardware item quoted in the RFP, the samples (except Servers) should be submitted to ELCOT indicating the make, model number and brochures / specification of the items for testing by ELCOT as per Annexure 8.2 (Sample Submission Form) of this RFP. ii. The pre – qualified bidders have to submit the samples (except Servers) within 7 days from the date of intimation from ELCOT unless any specific time given by ELCOT in writing.
2	Volume 1 - Page No. 47- Clause No. 5.4 Bid Evaluation Process - S.No. 2- Stage 2: Technical Proposal	v. Bidders should submit the samples as per the terms specified in Section 5.3 “Sample Submission Clause” initially to ELCOT and to SCRB for testing/evaluation. Preliminary sample evaluation will be done at ELCOT and the samples will be forwarded to SCRB for further evaluation. Based on the sample acceptance report from SCRB, the Technically qualified bidders will be selected under this tender for further process i.e. on the satisfactory comments/feedback from SCRB, the bidder will be selected as technically qualified bidder.	v. Bidders should submit the samples (except Servers) as per the terms specified in Section 5.3 “Sample Submission Clause” initially to ELCOT and to SCRB for testing/evaluation. Preliminary sample (except Servers) evaluation will be done at ELCOT and the samples (except Servers) will be forwarded to SCRB for further evaluation. Based on the sample acceptance report from SCRB, the Technically qualified bidders will be selected under this tender for further process i.e. on the satisfactory comments/feedback from SCRB, the bidder will be selected as technically qualified bidder.

3	Volume 1 - Page No. 136- Section 8.5 Annexure 5- Commercial proposal - 2. Pricing Formats - e. OPEX: Price Discovery- Subdivision 3- Data Centrer and Disaster Recovery Center	S.No. 1 Anti-virus Software for Servers and S.No. 2 Host Intrusion Prevention Software	Removed.
4	Volume 1 - Page No. 136- Section 8.5 Annexure 5- Commercial proposal - 2. Pricing Formats - e. OPEX: Price Discovery- Subdivision 3- Data centre and Disaster Recovery center		New items added. S.No. 1 Application Server (1 no.) and S.No. 2 Database Server (1 no.) are added.
5	Volume 1 - Page No. 129- Section 8.5 - Annexure 5- Commercial proposal - 2. Pricing Formats - a. CAPEX: DC/DRC/ Field Assests & Application Development- 1. CAPEX- DATA CENTER HARDWARE & 2. CAPEX - DISASTER RECOVERY CENTER HARDWARE		S.No. 1.4 - Anti-Virus Software (15 nos.) S.No. 1.5 - Host Intrusion Prevention Software (15 nos.) S.No. 2.3 - Anti-Virus Software (3 nos.) S.No. 2.4 - Host Intrusion Prevention Software (3 nos.) **Note:** **Antivirus and Host Intrusion Prevention Software are added in CAPEX and the bidder shall take care of overall maintenance including renewal of all licenses and updates till the expiry of the O&M period at no extra cost for all 18 Servers.**

6	Volume 1 -Page No. 129- Section 8.5 - Annexure 5- Commercial proposal - 2. Pricing Formats - 3. CAPEX - FIELD ASSEST HARDWARE - 3.4 - Inverter	Inverter - 1923 nos	Inverter - 1551 nos
7	Volume 1 - Page No. 134- Section 8.5 - Annexure 5- Commercial proposal - 2. Pricing Formats - e. OPEX: Price Discovery- Subdivision - 1. Site Infrastructure - 1) Site Preparation	S.No. 15 Installation - Electrical and S.No. 16 Installation - Network Components	Removed. **Note:** **Individual components S.No. 1 to 14 will be inclusive of Labour charges.**
8	Volume 1 - Page No. 135- Section 8.5 - Annexure 5- Commercial proposal - 2. Pricing Formats - e. OPEX: Price Discovery- Subdivision 2) Hardware items		New item added - S.No.3 Toner Cartridge is added.
9	Volume 1 - Page No. 72 & 73- Clause No. 7- Specification - 2. Existing Hardware Items	1) Online UPS Units:	1) Online UPS(2 KVA) Units: Make: Frontline & Model: FSS2000
		2) UPS Batteries:	2) UPS Batteries: Make & Model: Q42 Quanta Battery
10	Volume 1- Page No. 129- Section 8.5 - Annexure 5- Commercial proposal - 2. Pricing Formats - a. CAPEX: DC/DRC/Filed Assets & Application Development - 3. CAPEX - FIELD ASSETS HARDWARE- S.No. 3.2	UPS Units (Excluding Battery)	UPS (2KVA) Units (Excluding Battery)

11	Volume 1 - Page No. 66- Clause No. 7 Specification - 7) - Server Specification- S.No. 1 - Parameter - Processor	Latest series/ generation of 64-bit x86/ equivalent processor(s) with 16 or higher Cores Processor speed should be minimum 2.9 GHz and minimum 3.9 GHz turbo frequency, minimum 22MB Cache having SPEC Rate 2017_fp_base of 228 or Higher and SPEC Rate 2017_fp_base of 252 or Higher Minimum 2 processors per each physical server	Latest series/ generation of 64-bit x86/ equivalent processor(s) with 16 or higher Cores Processor speed should be minimum 2.9 GHz and minimum 3.9 GHz turbo frequency, minimum 22MB Cache having SPEC Rate 2017_fp_base of 228 or Higher and SPEC Rate 2017_int_base of 252 or Higher Minimum 2 processors per each physical server
12	Volume 1 - Page No. 27- Section No. 2.7 Technical Qualification - Criteria - D. Proposed Team - S.No. 1 to 4- Documentary Proof	1. The Bidder should provide CV (format provided in Annexure 8.4.3 (b) of all the below resources mentioning the projects handled along with experience meeting the requirements mentioned in Section 12 of Volume 2 of this RFP. Copy of documents confirming on roll status of the resources with bidder organization such as (Company ID Card, Aadhaar Card, EPF number, PAN, Email ID) 3. Flowchart and Detailed plan of resource deployment	The Bidder should provide CV (format provided in Annexure 8.4.3 (b)) of all the below resources mentioning the projects handled along with experience meeting the requirements mentioned in Section 12 of Volume 2 of this RFP. Copy of documents confirming on roll status of the resources with bidder organization such as Company ID Card & Company Email ID 2. Flowchart and Detailed plan of resource deployment
13	Volume 1 - Page No. 60- Section No. 7 Specification - 2) Online UPS with Battery - 2 KVA TRUE ONLINE UPS- Parameter 7. Battery (Secondary Source)	Sealed maintenance free (SMF) type – AH and no. of Batteries shall be suitably selected for the respective minimum backup time of 70% Resistive Load, 60 Minutes – 3160 VAH.	Sealed maintenance free (SMF) type – AH and no. of Batteries shall be suitably selected for the respective minimum backup time of 70% Resistive Load, 60 Minutes – 3000 VAH.

14	Volume 1 - Page No. 60- Section No. 7 Specification - 2) Online UPS with Battery - 5 KVA TRUE ONLINE UPS - Parameter 7. Battery (Secondary Source)	Sealed maintenance free (SMF) type – AH and no. of Batteries shall be suitably selected for the respective minimum backup time of 70% Resistive Load, 60 Minutes – 7900 VAH	Sealed maintenance free (SMF) type – AH and no. of Batteries shall be suitably selected for the respective minimum backup time of 70% Resistive Load, 60 Minutes – 7000 VAH
15	Volume 1 - Page No. 61- Section No. 7 Specification - 2) Online UPS with Battery - 5 KVA TRUE ONLINE UPS- Parameter 15 - Overload capacity	Overload Capacity: Withstand for 5 Minutes at 110% load (2200 Watts Resistive Load / 1540Watts Combinational Load).	Overload Capacity: Withstand for 5 Minutes at 110% load (5500 Watts Resistive Load / 1540Watts Combinational Load)
16	Volume 1 - Page No. 101- Section No. 5. Compliance to Minimum Hardware Specification - 2) Online UPS with Battery (2KVA): Parameter 18 - Ambient Temperature	To be specified by the tenderer (Preferable upto 50 Degree Celsius)	To be specified by the tenderer (Min 50 Degree Celsius)
17	Volume 2 - Page No. 225 - S.No. 19	Annexure 7- Application Security Requirements	Annexure 7- Application Security Requirements is replaced with Annexure 1 as enclosed
18	Volume 2- Page No. 134- Clause No. 8.10 - Business Continuity and Disaster Recovery -Pont No. 5	5) Replication between Data Centre and DR Site as well as changeover during disaster shall be quick for minimal impact on user experience. Ensuring data backup till the last transaction occurring in the system to ensure enhanced service levels. RPO and RTO objectives are as below and shall be strongly adhered to. RPO = 0 minutes RTO <=60 minutes	Replication between Data Centre and DR Site as well as changeover during disaster shall be quick for minimal impact on user experience. Ensuring data backup till the last transaction occurring in the system to ensure enhanced service levels. RPO and RTO objectives are as below and shall be strongly adhered to. RPO <15 minutes RTO <=60 minutes (The network requirement for connectivity between DC and DRC to achieve the objective shall be assessed

			by the bidder)
19	Volume 2 - Page No. 157- Clause No. 8.20 - Operation and Maintenance - Overall System- Point No. 1	Undertake preventive maintenance (any maintenance activity that is required before the occurrence of an incident with an attempt to prevent any future incidents) and carry out the architecture changes wherever needed to keep the performance levels of the hardware and equipment in tune with the requirements of the SLA. Such preventive maintenance shall not be performed during peak working hours of SCRB, unless inevitable and approved in advance by the SCRB.	Undertake preventive maintenance (any maintenance activity that is required before the occurrence of an incident with an attempt to prevent any future incidents) and carry out the architecture changes once in every 6 months to keep the performance levels of the hardware and equipment in tune with the requirements of the SLA. Such preventive maintenance shall not be performed during peak working hours of SCRB, unless inevitable and approved in advance by the SCRB
20	Volume 2- Page No. 60- Clause No. 7.1.6 - Scope of Work Overview- S.No. 7- Integration with External Databases - Module	b) Personal Identity Databases like Aadhaar, Voter ID, Ration Card, Passport, PAN etc.	b) Personal Identity Databases like Aadhaar, Voter ID, Ration Card, Passport, PAN etc. (SCRB will facilitate for accessing aadhaar data. **However Bidder has to provide HSM system for storing encryption keys**. The transactional cost, if any will be borne by SCRB)
21	Volume 2 - Page No. 46 - Clause 6.2.10.2 - Data Center / Disaster Recovery Center.	For details regarding the server count, please refer below table:	Removed along with the Table containing details of servers at ELCOT SDC and DR, Pune.

22	Volume 2 - Page No. 44- Clause No. 6.2.9 Helpdesk & Incident Management	The Helpdesk support team shall be deployed at SCRB and work closely with PMU and divisional staff of the project to resolve issues. SI may deploy additional resources based on the need of the project and also meet the defined SLAs defined in the RFP.	The Helpdesk support team shall be deployed at SCRB and work closely with PMU and divisional staff of the project to resolve issues. SI may deploy additional resources based on the need of the project and also meet the defined SLAs defined in the RFP. Helpdesk shall be operational 16X7X365 (06.00 am to 10.00 pm). SI to ensure atleast 2 seats to operational during the support window. Helpdesk shall be operational through service desk portal & through mobile call reporting. Desktops, Printer, Scanner, LAN, UPS Power, Furniture and space for helpdesk will be provided by SCRB.
23	Volume 3 - Page No. 9 -Clause No. 1. Definition and Interpretation - 1.2 Interpretation – Point No. 16	"**Contract/ Project Period**" means the time period from the date of signing of Contract till 5 years after Go-live or further extended on mutually agreed basis.	"**Contract/ Project Period**" means the time period from the date of signing of Contract till 5 years after Go-live or further extended (not exceeding 1 year) till alternate arrangement is done by the SCRB to manage the operations.
24			Clarification to queries are enclosed in Annexure-2

Note: The above corrigendum is applicable to all other clauses, which contain the respective terms in the tender document.

Managing Director

Annexure 1

Application Security Requirements

1.1 Endpoint protection			
S No.	**Minimum Specifications**	**OEM Compliance (Yes/No)**	**Cross Reference Document/Links**
	Make: Model:		
1	The proposed solution should be positioned in the leader quadrant from last three published Gartner Magic quadrant report for Endpoint Protection		
2	Endpoint solution should have capability of AV, Vulnerability Protection, Firewall, Device control, Application Control, Virtual Patching, DLP from day one.		
3	Proposed solution should have Pre, Post and Runtime machine learning capability		
4	Proposed solution should have True file type scan along with Proactive outbreak prevention and Command & Control callback detection		
5	File reputation - Variant protection - Census check - Web reputation		
6	Advanced malware and ransomware protection: Defend endpoints—on or off the corporate network—against malware, Trojans, worms, spyware, ransomware, and adapts to protect against new unknown variants and advanced threats like crypto malware and fileless malware		
7	Endpoint vulnerability protection should scan the machine and provide CVE number visibility and accordingly create rule for virtual patch against vulnerability		
8	Behavior monitoring along with ransomware protection engine, ransom ware engine should have feature to take backup of ransom ware encrypted files and restoring the same		
9	Proposed solution should have IPv4 and IPv6 support		
10	Endpoint solution should have data loss prevention with pre-defined templates for HIPAA, PCI-DSS, GLBA etc. for compliance requirements and should have capability to create policies on basis of regular expression, key word and dictionary based		
11	Offers visibility and control of data in motion of sensitive information—whether it is in email, webmail, instant messaging (IM), SaaS		

	applications, and most networking protocols such as FTP, HTTP/HTTPS, and SMTP		
12	Prevents potential damage from unwanted or unknown applications (executables, DLLs, Windows App store apps, device drivers, control panels, and other Portable Executable (PE) files)		
13	Provides global and local real-time threat intelligence based on good file reputation data correlated across a global network		
14	Contains broad coverage of pre-categorized applications that can be easily selected from application catalog (with regular updates)		
15	Uses application name, path, regular expression, or certificate for basic application whitelisting and blacklisting		
16	Uses intelligent and dynamic policies that still allow users to install valid applications based on reputation-based variables like the prevalence, regional usage, and maturity of the application		
17	Ensures that patches/updates associated with whitelisted applications can be installed, as well as allowing your update programs to install new patches/updates, with trusted sources of change		
18	Should have roll-your-own application whitelisting and blacklisting for in-house and unlisted applications		
19	Limits application usage to a specific list of applications supported by data loss prevention (DLP) products for specific users or endpoints and collects and limits application usage for software licensing compliance		
20	Proposed solution should not send any file/sample with cloud to inspect and analyze for any threat		
21	Features system lockdown to harden end-user systems by preventing new applications from being executed		
22	Should be capable of recommending rules based on vulnerabilities on endpoint and create dynamic rules automatically based on System posture and endpoint posture		
23	Blocks known and unknown vulnerability exploits before patches are deployed and Provides protection before patches are deployed and often before patches are available		
24	Vulnerability Protection virtually patches known and unknown vulnerabilities, giving you instant protection, before a patch is available or deployable		
25	Automatically assesses and recommends		

	required virtual patches for your specific environment		
26	Dynamically adjusts security configuration based on the location of an endpoint		
27	Blends signature-less techniques, including high-fidelity machine learning, behavioral analysis, variant protection, census check, application control, exploit prevention, and good file check with other techniques like file reputation, web reputation, and command and control (C&C) blocking		
28	Shields operating system and common applications from known and unknown attacks		
29	Organizes vulnerability assessments by Microsoft security bulletin numbers, CVE numbers, or other important information		
1.2 Server Security (Host Intrusion Prevention System)			
S No.	**Minimum Specifications**	**OEM Compliance (Yes/No)**	**Cross Reference Document/Links**
	Make: Model:		
1	The solution must provide single platform for complete server protection over physical, virtual (server/desktop), & cloud:		
2	Complete protection from a single integrated platform: addresses all of the 'Gartner top ten server security priorities'		
3	Provides layered defense against advanced attacks and shields against known and unknown vulnerabilities in web and enterprise applications and operating systems.		
4	Single management console to manage workloads across physical, virtual and cloud		
5	The proposed solution must be able to perform machine learning to discover new threats before file is executed		
6	The proposed solution must be able to monitor behavior of running process to detect malicious behaviors		
7	The Proposed Solution Should Support Behavior Monitoring		
8	The Proposed Solution Should Support Realtime monitoring and should be able to detect and clean malware even if it is stagnant and not executing		
9	The proposed Solution should be able to Detect Malware at Disk IO		
10	The Proposed Solution Should support Manual and Scheduled Scans.		

11	Must be able to provide scan assessment engine to discover OS & application vulnerabilities on a server and determine which vulnerabilities have not been mitigated & recommend rules to shield to shield applications & systems with advanced deep packet inspection technology		
12	Must feature a high-performance deep packet inspection engine that examines all incoming and outgoing traffic for protocol deviations, content that signals an attack, or policy violations		
13	Must be able to operate in detection or prevention mode to protect operating systems and enterprise application vulnerabilities		
14	Must provide detailed events with valuable information, including who attacked, when they attacked, and what they attempted to exploit. Administrators can be notified automatically via alerts when an incident has occurred		
15	Must be able to provide protection against known and zero-day attacks		
16	Must include smart rules to provide zero-day protection from unknown exploits that attack an unknown vulnerability, by detecting unusual protocol data containing malicious code		
17	Must include exploit rules to stop known attacks and malware and are similar to traditional antivirus signatures in that they use signatures to identify and block individual, known exploits		
18	Must automatically shield newly discovered vulnerabilities within hours, pushing protection to large number of servers in minutes without a system reboot		
19	Must be able to provide Application Control in whitelist or blacklist mode		
20	Solution should support adding of Blacklisted IOC's (Hashes) for Blocking		
21	Solution should have the ability to work in Detect and Block mode		
22	Solution should have the ability to show all the running processes and give the option for Allow or Block in intuitive GUI		
23	The solution should support Maintenance Mode in which during predefined Downtimes, upgrade etc. can take place and all processes automatically learnt and Whitelisted		
24	Must include an enterprise-grade, bidirectional stateful firewall providing centralized management of firewall policy, including predefined templates		
25	Detection of reconnaissance scans		
26	Solution Should support Inline and TAP Modes		

27	Solution should be able to Configure Stateful and Stateless		
28	Solution Should support SSL Decryption		
29	Must be able to monitor critical operating system and application such as directories, registry keys, and values to detect and report malicious and unexpected changes in real-time		
30	Solution Should Support Realtime Integrity Monitoring		
31	Solution Should support Integrity Monitoring for Process, Ports, Files, Attributes, Permissions		
32	Solution should enable IM rules based on the posture of the machine and should be dynamic (Like new software installed)		
33	The proposed solution should have intelligence to analyze and share key informational events for correlation to SIEM		
34	The proposed solution should be positioned in the leader quadrant from last three published Gartner Magic quadrant report for Endpoint Protection		
1.3 Advanced Email Security Gateway with ATP			
S No.	**Minimum Specifications**	**OEM Compliance (Yes/No)**	**Cross Reference Document/Links**
	Make: Model:		
1	The proposed OEM must be positioned in Leader Quadrant " The Forrester Wave Enterprise Email Security, Q2 2019 Report".		
2	The proposed solution should be a appliance based dedicated Email Anti-APT Security solution that provides enterprise message transfer agent (MTA) capabilities SMTP/SMTP-TLS, Antimalware, BEC/CEO fraud attack prevention, social engineering attack protection, ransomware, unknown malware threats - Sandboxing and anti-phishing.		
3	solution should support domain authentication using DMARC and spam prevention using DKIM and Sender policy Framework		
4	Simplifies regulatory compliance and data loss prevention through pre-defined and customizable DLP policies and templates		
5	The proposed solution must be purpose-built hardware appliance with hardened operating system and must be able to support both incoming as well as outgoing messages.		

6	The solution must have SMTP Traffic Throttling to block messages from a single IP address or sender for a certain time when the number of connections or messages reaches the specified maximum. Also provide Firewall against DHA and bounced mail attacks.		
7	The proposed solution must have dedicated management port which should be separate from data ports.		
8	The proposed solution should be a hardware appliance with redundant power supply.		
9	Deployment mode: Solution must support flexible deployment modes -MTA, BCC, SPAN/TAP modes.		
10	Solution must be able to analyze, process and inspect at least 400,000 emails/day.		
11	File Types Supported : Multiple file types including windows executables, Scripts, Java, office, office with macros, Pdf, image/jpeg files, vbs, dll, lnk, swf All types of Compressed files.		
12	Solution must support file size support up to 50 MB in case of sandboxing.		
13	Solution should support IPv4 and IPv6 addressing for email message processing and management console and CLI access.		
14	Solution must support at least 25 or more sandboxing virtual instances on the email APT appliance to provide consolidated inspection of emails with low false positive rates.		
15	Solution must be capable to sandbox file as well as URL's.		
16	The proposed solution must support both 32-bit / 64-bit Windows 8 ,8.1 & 10, Windows 2003 ,2008 & 2016 server sandbox images and should allow at least three types of sandbox images for virtual analysis.		
17	The proposed solution should investigate URLs embedded in an email message by using reputation technology, direct page analysis, and sandbox simulation if required.		
18	The proposed solution support advanced detection technology to discover targeted threats in email messages, including spear-phishing and social engineering attacks. • Reputation and heuristic technologies catch unknown threats and document exploits • File hash analysis blocks unsafe files and applications • Detects threats hidden in password-protected files and shortened URLs • Predictive machine learning technology detects		

	emerging unknown security risks		
19	The proposed solution should have capability to uses advanced machine learning technology to correlate threat information and perform in-depth file analysis to detect emerging unknown security risks.		
20	The Proposed solution should be able to detect and analyze URLs which embedded in MS office and PDF attachments.		
21	The proposed solution should have anti-malware and anti-spam engine		
22	The proposed solution should look for known and potential exploits to the intended office application and analyze macros		
23	The Proposed solution detect and analyze the URL direct link which point to a file on the mail body.		
24	The Proposed solution should be able to detect and analyzed the URL's in mail subject.		
25	The Proposed Solution should be able to detect known bad URL before sandboxing		
26	The proposed solution should be able to detects, downloads and analyzes files directly linked in the email message body.		
27	The Proposed solution should be able to detect true file types.		
28	The Proposed solution should have capabilities to detect Ransomware using Decoy files on sandboxes.		
29	The Proposed solution should not have any limitation which require all attachments to be sent to sandbox, only suspicious attachments should be sent to sandbox for analysis.		
30	The Proposed solution should have an option for timeout/ release of an email if the file analysis on the sandbox is taking over 20 mins.		
31	The Proposed solution should support heuristically discovery passwords in email messages or import custom password for inspecting email messages with password protected file.		
32	The Proposed solution should support at least 100 predefined passwords for scanning archive files		
33	The solution should be able to Block mail message and store a copy in the quarantine area.		
34	The Proposed solution should be able to Deliver the email message to the recipient after replacing the suspicious attachments with a text file and tag the email message subject with a string to notify the recipient		

35	The Proposed solution should be able to pass and tag the email message		
36	The Proposed solution should have option to make policy exceptions for safe senders, recipients, and X-header content, files and URL's		
37	The Proposed Solution should be able to define risk levels after investigation of email messages		
38	The Proposed solution should allow administrators to be able to see the HTML format reporting on console and download PDF report		
39	The Proposed solution should be able to send real time email alert per detection		
40	The Proposed Solution should support Real-Time URL click protection.		
41	The Proposed Solution should support manual email message submission in" .eml" format for analysis purpose.		
42	The Proposed Solution should support Pre-Execution Machine Learning scanning feature which looks at static file features to predict maliciousness in mail & attachment in the mail.		
43	Solution should have an option to generate reports on demand or set a daily, weekly, or monthly schedule.		
44	The proposed solution should support on premise centralized management for viewing information about detection, message tracking and MTA logs.		
45	Solution should be able to integrate with Microsoft Active Directory (AD) for account management		
46	Solution should be able to centrally manage and deploy product updates including patches, hotfixes, and firmware upgrade		
47	The solution central management should include various methods of sharing threat intelligence data with other products or services including TAXII / Web services.		
48	Solution must support custom intelligence i.e. STIX/TAXII, IOC's, YARA and create suspicious objects repository for Organization.		

Annexure 2

Clarifications

S. No	Title of the Clause	Tender Clause	Clarification requested	Clarification
1	Volume 1 - Page No. 62- Section No. 7 Specification- - 2) Online UPS with Battery - Parameter 33 - Other Features	Minimum Specification - Online UPS 2KVA & 5 KVA.	Pl clarify if only SNMP slot to be provided or along with the card to be provided	SNMP slot along with SNMP Card shall be provided for both 2KVA & 5KVA Online UPS.
2	Volume 2 - Page No. 90- Clause No. 7.3.12 - Communication Module -SI Scope of Work - FR 1 - Functional Requirement	The system should have 2 modes of email triggers: Manual mode and Autotrigger mode	Please specify whether TN Police will provide the email gateway procured by them to be used for integration or not	SMS, email and payment gateways shall be provided by SCRB for integration.
3	Volume 2 - Page No. 107- Clause No. 7.4.7 - Mobile Application Development	The SI should develop a mobile application which should be compatible with Android OS latest version.	Please specify whether only Android version is needed or separate iOS version is also expected here	Application shall be available in popular OS version such as Android, iOS, ipad OS etc.
4	Volume 2 - Page No. 39- Clause No. 6.2.2 - Site Preparation	As mentioned in Section 6.1.1 above, an estimated 15% of the premise infrastructure items which include cabling, network racks & switches, earthing, etc. are damaged or in poor condition. Hence, as part of CCTNS 2.0 site preparation scope of work, such items have to be checked for faults, replaced or rectified	Please clarify, once site preparation is completed and signed off from SHO. Incase of any damage due to mishandling (or) entire PS short circuit, (or) rodent bite. Whether the additional charges to be taken care by respective PS	Physical damages due to mishandling or short circuit or rodent bite will be taken care by SCRB/PS.
5	Volume 2 - Page No. 210- Clause No. 14.2 - General Requirement for Application	General Requirement of application	Is the solution/web portal expected to be in English only or it needs to be in any regional language like Tamil.	Application shall be developed in both Tamil & English.