ELCOT Adding Value through IT	**Electronics Corporation of Tamil Nadu Limited**
Tender	**Supply, Installation, Commissioning and Maintenance of Hardware for CSA-TN** **Tender Ref.** **ELCOT/Proc/OT/33331/Hardware for CSA-TN/2020-21**
	Corrigendum No. 2 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	To be Read as
1	Page No. 29- Section 5-Specifications- Item code - 33331-006 SAN Storage- Backup Appliance Specification- S.No. 29	Proposed disk based backup appliance should be able to interface with various industry leading server platforms, operating systems and Must support LAN/SAN based D2D backup and VTL backup simultaneously via NFS v3, CIFS, FC , OST and NDMP protocols.	Proposed disk based backup appliance should be able to interface with various industry leading server platforms, operating systems and Must support LAN/SAN based D2D backup and backups to be configured simultaneously via NFS v3, CIFS, FC and integrate with application that use OST , NDMP and equivalent capabilities.
2	Page No. 29- Section 5-Specifications- Item code - 33331-006 SAN Storage- Backup Appliance Specification- S.No. 31	Proposed appliance should be offered with protocols like VTL, OST, CIFS and NFS. All of the protocols should be available to use concurrently with global deduplication for data ingested across all of them.	Proposed appliance/solution should be offered with protocols like OST, CIFS and NFS. All of the protocols should be available to use concurrently
3	Page No. 31- Section 5-Specifications- Item code - 33331-006 SAN Storage- Backup Appliance Specification- S.No. 53	Bidder should Capacity/Socket based license with no limit to the count of servers/DB to backup. SI need to provide backup solution on the offered IT Infra stack from single OEM for backup software & purpose built backup appliance.	Bidder should Capacity/Socket based license with no limit to the count of servers/DB to backup. SI need to provide backup solution on the offered IT Infra stack from single OEM for backup software & purpose built backup appliance. (Note: Currently 12 physical server with Dual socket are in place)
4	Page No. 21- Section 5-Specifications- Item code - 33331-002 - Layer 3 Switch -Specification- S.No. 12- Security	The Switch should support IEEE 802.1X and RADIUS network logins	The Switch should support IEEE 802.1X / RADIUS /equivalent network logins
5	Page No. 15- Clause No. 4 Eligibility Criteria – S.No. 7	The bidder and Hardware OEMs should have a service centre in Chennai.	Bidder/Hardware OEMs should have a service centre in Chennai.
6	Page No. 22- Section 5-Specifications- Item code - 33331-003 – Firewall-	Should have min 16 Gb RAM in both primary & HA firewalls	Should have Min 8 Gb RAM in both primary & HA firewalls

	S.No. 3- Hardware & Interface Requirement		
7	Page No. 22 - Section 5-Specifications- Item code - 33331-003 – Firewall- S.No. 3- Hardware & Interface Requirement	Should have minimum 500 GB of Hard disk/SSD both primary & HA firewalls	Should have minimum 500 GB (Integrated/External) of Hard disk/SSD both primary & HA firewalls
8	Page No. 23 -Section 5-Specifications- Item code - 33331-003 – Firewall- S.No. 4- Security Operational Requirement	Anti-Bot and Anti-Virus application must have a centralized event correlation and reporting mechanism	Anti-Bot and Anti-Virus application must have a centralized reporting mechanism
9	Page No. 23- Section 5-Specifications- Item code - 33331-003 – Firewall- S.No. 4- Security Operational Requirement	Solution should support detection& Prevention attack types ie, such as spam sending click fraud or self-distribution, that are associated with bots	Solution should support Anti Spam detection & prevention attacks.
10	Page No. 23 - Section 5-Specifications- Item code - 33331-003 – Firewall- S.No. 4- Security Operational Requirement	The Anti-Virus should support scanning for links inside emails	The Anti-Virus should support scanning and detection of malware in emails
11	Page No. 47 - Section 5-Specifications- Item code - 33331-010- Distributed Denial of Service (DDoS)- S.No. H. Certification / References	Device should be Common criteria certified at least EAL 3 or equivalent	Device should be Common criteria certified at least EAL3/FCC/VCCL or equivalent
12	Page No. 28- Section 5-Specifications- Item code - 33331-006 - SAN Storage- S.No. 19	The Storage array must support capability to replicate data to remote site array in synchronous and asynchronous modes. This license should be configured for entire supported capacity of the array and the proposed storage should be configured to replicate with the DR storage.	The Storage must support capability to replicate data to remote site storage in synchronous or asynchronous modes.
13	Page No. 29- Section 5-Specifications- Item code - 33331-006 - SAN	Proposed appliance should support industry leading backup software like EMC Networker, Symantec	Proposed appliance / integrated appliance should support deduplication at backup server/ host / application level so that

	Storage - Backup Appliance Specification- S.No. 32	Netbackup, Commvault and HP Data Protector etc and should Support deduplication at backup server/ host / application level so that only changed blocks travel through network to backup device	only changed blocks travel through network to backup device.
14	Page No. 24 - Section 5-Specifications- Item code - 33331-003 – Firewall- S.No. 5. Management, Forensics & Reporting	Reporting & Analyser Solution should have min 3000 log/sec sustained & indexed , min 1 TB HDD & 16 GB Memory	Reporting & Analyser Solution should have min 3000 log/sec sustained & indexed , min 1 TB HDD & Min. of 8 GB Memory
15	Page No. 35- Section 5-Specifications- Item Code 33331-009 - Web Application Firewall - S.No. A. General	The proposed solution should have at least 4 virtual instances to run separate WAF licenses for different applications and it should be upgradeable to 8 or higher	The proposed solution should have at least 4 virtual instances / domains to run separate WAF licenses for different applications with complete isolation between applications and it should be upgradeable to 8 or higher
16	Page No. 35 - Section 5- Specifications- Item Code 33331-009 - Web Application Firewall - S.No. A. General	Each virtual instances should be complete independent in nature with separate routing table, ARP table, session table etc	Each virtual instances/domains should be completely independent in nature
17	Page No. 35- Section 5-Specifications- Item Code 33331-009 - Web Application Firewall- S.No. A. General	Proposed solution should have at least 5 Gbps of throughput and scalable to 10 Gbps or higher	Proposed solution should have at least 5 Gbps of WAF throughput and scalable to 10 Gbps or higher
18	Page No. 41- Section 5-Specifications- Item Code 33331-009 - Web Application Firewall- S.No. D. Web Application Firewall Features	The solution should be IPv6/ IPv4 dual stack compatible with IPv6 certified.	The solution should be IPv6/ IPv4 dual stack compatible
19	Page No. 41- Section 5-Specifications- Item Code 33331-009 - Web Application Firewall- S.No. E. Reporting Features	The system must provide request logging that support profile by enabling configuration log entries to be reported when requests/ responses are received, supports audit logging of HTTP/decrypted HTTPS requests/responses, and enables	The system must provide request logging that support profile by enabling configuration log entries to be reported when requests/ responses are received, supports audit logging, and enables specification of a response to be issued when a specific requests/responses occur.

		specification of a response to be issued when a specific requests/responses occur.	
20	Page No. 44 - Section 5-Specifications- Item Code 33331- 010 -Distributed Denial of Service (DDoS) - S.No. B. Generic Features	The solution should be IPv6/ IPv4 dual stack compatible with IPv6 certified.	The solution should be IPv6/ IPv4 dual stack compatible
21	Page No. 44- Section 5-Specifications- Item Code 33331- 010 -Distributed Denial of Service (DDoS) - S.No. C. Security / DDoS Feature	System should support horizontal and vertical port scanning behavioral protection	System /Solution should support horizontal and vertical port scanning behavioral protection
22	Page No. 45 - Section 5-Specifications- Item Code 33331- 010 - Distributed Denial of Service (DDoS) - S.No. C. Security / DDoS Feature	System should Protect from Brute Force and dictionary attacks	System/Solution should Protect from Brute Force and dictionary attacks
23	Page No. 45 - Section 5-Specifications- Item Code 33331- 010 - Distributed Denial of Service (DDoS) - S.No. C. Security / DDoS Feature	System should support suspension of traffic/ blacklisting from offending source based on a signature/attack detection	System /Solution should support suspension of traffic/ blacklisting from offending source based on a signature/attack detection
24	Page No. 45 - Section 5-Specifications- Item Code 33331- 010 - Distributed Denial of Service (DDoS) - S.No. C. Security / DDoS Feature	System should support intrusion prevention from known attacks either on the appliance or through external appliance	System/Solution should support intrusion prevention from known attacks either on the appliance or through external appliance
25	Page No. 45 - Section 5-Specifications- Item Code 33331- 010 - Distributed Denial of Service (DDoS) - S.No. C. Security / DDoS Feature	System should have capability to allow custom signature creation	System/Solution should have capability to allow custom signature creation
26	Page No. 48 - Section 5- Specifications- Item Code 33331- 011 - Security Information and Event Management – S.No.	Proposed solution should extract the attributes of a network session in the form of a meta [Like IP source, Destination, Country, Mac Address etc…] from both	Proposed solution should extract the attributes of a network session in the form of a meta [Like IP source, Destination, Country, Mac Address etc…] from both header and payload

	2. Log Collection and Management	header and payload of all common network protocols	
27	Page No. 49 - Section 5-Specifications- Item Code 33331- 011 - Security Information and Event Management- S.No.3. Correlation	D. Spear Phishing : Proposed Solution should reconstruct network protocols on the wire and can extract and analyze files being transferred. Combining this with deep file inspection, file anomalies signifying potentially malicious executable delivery can be alerted on and investigated. Spear phishing is a common delivery mechanism employed by attackers, often times carrying malicious files (eg. Encrypted executables, weaponized PDFs). E. Dynamic DNS - Data Exfiltration : Proposed Solution should reconstruct network protocols on the wire and can extract and analyze files being transferred. A common data exfiltration technique used by threat actors involves uploading archive files to external hosts using dynamic DNS domains. Proposed Solution can extract the root domain for dynamic DNS providers and detect uploads (eg. HTTP upload) of data and uncover the impact to business F. Malicious Protocols - Ghost RAT : Many commonly used remote access tools (RATs) have been programmed with custom network protocols in an effort to evade detection by traditional tools. Proposed solution should support through full session reconstruction and deep inspection into network traffic, is able to detect the Gh0st RAT protocol in real- time	D. Spear Phishing : Proposed Solution should reconstruct, can extract and analyze files being transferred. Combining this with deep file inspection, file anomalies signifying potentially malicious executable delivery can be alerted on and investigated. Spear phishing is a common delivery mechanism employed by attackers, often times carrying malicious files (eg. Encrypted executables, weaponized PDFs). E. Dynamic DNS - Data Exfiltration : Proposed Solution should reconstruct, can extract and analyze files being transferred. A common data exfiltration technique used by threat actors involves uploading archive files to external hosts using dynamic DNS domains. Proposed Solution can extract the root domain for dynamic DNS providers and detect uploads (eg. HTTP upload) of data and uncover the impact to business F. Malicious Protocols - Ghost RAT : Many commonly used remote access tools (RATs) have been programmed with custom network protocols in an effort to evade detection by traditional tools. Proposed solution should support through full session reconstruction and deep inspection into network traffic, is able to detect the Gh0st RAT protocol in real- time
28	Page No. 51 - Section 5-Specifications-	The solution should provide network traffic insight by	The solution should provide network traffic insight by

	Item Code 33331- 011 - Security Information and Event Management- S.No. 8. Real-Time and Advanced Analytics	a. Classifying protocols and applications b. Reconstructed file such as a Word document, image, Web page, system files c. Deep-packet inspection d. Log Analysis & Aggregation e. Reconstruct sessions and analyze artifacts f. Preview artifacts and attachments	a. Classifying applications b. Reconstructed file such as a Word document, image, Web page, system files c. Deep-packet inspection d. Log Analysis & Aggregation e. Reconstruct file and analyze artifacts f. Preview artifacts and attachments
29	Page No. 25- Section No. 5- Specification- Item code: 33331-004 IP KVM Switch – S.No. 10.	Hot Swappable Power Supply (without turning on/off KVM)	Redundant Power Supply
30	Page No. 15- Section No. 4. Eligibility Criteria – S.No. 8	**Eligibility Conditions:** Hardware OEM/s should have ISO 9001:2015 or latest certified manufacturing facility and ISO 14001:2015 or latest certified for handling hazardous products. **Documentary Proof to be submitted:** Should submit copy of VALID ISO 9001: 2015 or latest and ISO 14001: 2015 or latest Certificates of OEM/s.	**Eligibility Conditions:** OEM/s should have ISO 9001:2015 or latest certified manufacturing facility / 27001: 2013 or latest for Information Security Management System AND/OR ISO 14001:2015 or latest certified for handling hazardous products. **Documentary Proof to be submitted:** Should submit copy of VALID ISO 9001: 2015 or latest/ 27001: 2013 or latest AND/OR ISO 14001: 2015 or latest Certificates of OEM/s.
31	Page No. 18- Section No. 5- Specification- Item code: 33331-002 - Layer 3 Switch- S.No. 5 Resiliency and high availability	The Switch should support Bidirectional Forwarding Detection (BFD) to enables link connectivity monitoring and reduces network convergence time for RIP, OSPF, BGP, VRRP and switch virtualization technology	The Switch should support Bidirectional Forwarding Detection (BFD) to enables link connectivity monitoring and reduces network convergence time for OSPF, BGP, VRRP and switch virtualization technology
32	Page No. 19- Section No. 5- Specification- Item code: 33331-002 - Layer 3 Switch- S.No. 9 Layer3 IPv4 routing	The Switch should support static routes, RIP and RIPv2, OSPF, BGP	The Switch should support static routes, OSPF, BGP
33	Page No. 19- Section No. 5- Specification- Item code: 33331-002	The Switch should enables link connectivity monitoring and reduces network convergence	The Switch should enables link connectivity monitoring and reduces network convergence

	Layer 3 Switch- S.No. 9- Layer3 IPv4 routing	time for RIP, OSPF, BGP, VRRP	time for OSPF, BGP, VRRP
34	Page No. 22- Section No. 5- Specification- Item code: 33331-003 Firewall- S.No. 4- Security Operational Requirement	The solution must have ability to inspect all network traffic in a single policy to protect against threats including vulnerability exploits, viruses, spyware and data leakage	The solution must have ability to inspect all network traffic in security policies to protect against threats including vulnerability exploits, viruses, spyware

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

- SD/-

Managing Director