MAHATRANSCO
Maharashtra State Electricity Transmission Co. Ltd.

MAHARASHTRA STATE ELECTRICITY TRANSMISSION CO. LTD.
(CIN No. U40109MH2005SGC153646)

Name of Office: Central Purchase Agency,
Office Address: Prakashgad, 1st Floor, Plot No. G-9, Anant Kanekar Marg, Bandra (East),
Mumbai-51
Contact No.: 022-26474211/26472131
Email Id: cecpa@mahatransco.in
Website: www.mahatransco.in

SP/T-0703/0322 Date: 23.06.2022

AMENDMENT NO.-IV

Sub: Supply, Installation, Commissioning, Testing & Integration of Cyber Security Tools for MSLDC Kalwa, ALDC Ambazari and MSETCL Corporate Office at BKC, Bandra against e-Tender No. SP/T-0703/0322 [RFx No. 7*22437] **- Issue of Clarification / Amendment to tender document in response to Bidder's queries and extension in due date of submission and opening of bid.**

****

Please refer e-Tender No. SP/T-0703/0322 [RFx No. 7000022437], advertised for Supply, Installation, Commissioning, Testing & Integration of Cyber Security Tools for MSLDC Kalwa, ALDC Ambazari and MSETCL Corporate Office at BKC, Bandra.

In response to above tender, the **Clarification / Amendment to Tender specifications on** bidder's queries are given in Annexure - C enclosed herewith.

Considering the above, the due dates of submission and opening of Tender are hereby modified as under:

Due date and time of submission of bids	: 29.06.2022 up to 17.00 Hrs.
Due date and time of opening of bids	: 29.06.2022 at 17.15 Hrs.

All participant bidders are requested to take note of the above and submit their bids accordingly. All other terms and conditions of the Tender specifications remain unchanged.

- sd -
Executive Engineer (St.-VII)

ANNEXURE C

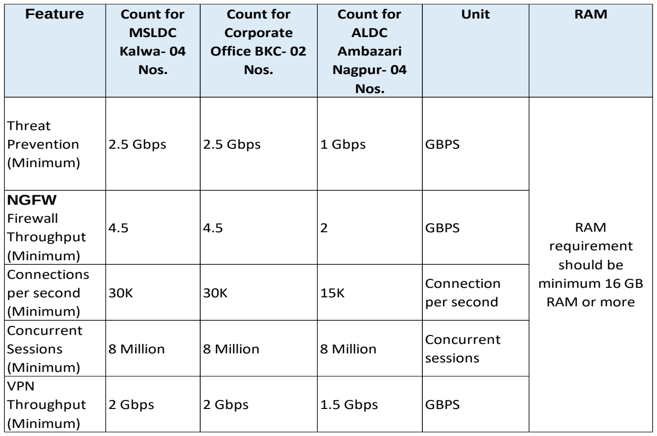
Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL							
Sr. No.	Vendor	No.	Page No., Clause No.	Description	Vendor		MSETCL
					Querry/Clarification	Changes Required	Revisions & Comments
1	Check point	6.2.1 Anti-APT Sizing	Page No-18 Maximum volume of processed traffic (Mbps) Minimum RAM (GB) Minimum number of logical cores	MSLDC Kalwa: 10 Corporate Office, BKC: 10 ALDC, Ambazari, Nagpur: 05-08	Need clarification on Sizing as Anti-APT sizing is based on throughput and no of file scan capability. Aslo every OEMs propose hardware or cloud solution for Anti-APT hence defineing the compute size is not relevent in Anti=Apt solution	Request to change clasue as "Anti-APT solution must have minimum 10Mbps of thoroughput and scalable upto 1Gbps for each locations"	**Revised Clause:** Anti-APT solution must have minimum 10Mbps of thoroughput for Kalwa and BKC Locations and Minimum 5 Mbps for ALDC Ambazari, and scalable upto 500 Mbps for each locations & should have minimum 8 VM
2	Check point	6.2.2 Anti-APT solution specifications	Page No-18 Clause No 1	The Anti-APT solution offered must be rated as ‘leaders’ or 'Challengers' in the Gartner Magic Quadrant published by Gartner from last three years.	There is no Gartner report for Anti-APT solution hence request to remove the clause.	Request to delete the clause	**Revised Clause:** The Anti-APT solution offered must be rated as Top Player or specialist in Redicati APT production quadrant published by Redicati in any of last 3 years or Anti-APT solution operating system must be NIAP (National Information Assurance Partnership) Common Criteria certified.

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL							
Sr. No.	Vendor	No.	Page No., Clause No.	Description	Vendor		MSETCL
					Querry/Clarification	Changes Required	Revisions & Comments
3	Check point	6.2.2 Anti-APT solution specifications	Page No-19 Clause No 29	Solution should be capable to integrate with devices link Enterprise Antivirus product to mitigate risk by blocking similar threat by pushing hashes/signature.	Due to this clause we are unable to participate in Bid and moreover this clause is favoring Antiviors vendors hence request to remove this clasue.	Request to delete the clause	To be Removed

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	No.	Page No., Clause No.	Description	Vendor		MSETCL
					Querry/Clarification	Changes Required	Revisions & Comments
4	Check point	6.4.2 EDR Specifications	Page No-25 Clause No 1	The EDR solution offered must be rated as ‘leaders’ or 'Challengers' in the Gartner Magic Quadrant published by Gartner from last three years.	There is no Gartner report for EDR solution. Only MITRE evaluate the perfromance of EDR solution Hence request to change clause as "The EDR solution offered must be rated as ‘leaders’ or 'Challengers' in the MITRE Engenuity ATT&CK® Evaluations published by MITRE."	The EDR solution offered must be rated as ‘leaders’ or 'Challengers' in the MITRE Engenuity ATT&CK® Evaluations published by MITRE.	**Revised Clause:** The EDR solution offered must have detection rate of more than 80% or more as per MITRE Engenuity ATT&CK® Evaluations published by MITRE 2022 or Should be listed as 'Leaders' or 'Strong Performers' in The Forrester Wave Report in atleast any one of the last three years as published by Forrester Research Inc.

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	No.	Page No., Clause No.	Description	Vendor		MSETCL
					Querry/Clarification	Changes Required	Revisions & Comments
5	Check point	6.5.1 Firewall Sizing	Page No-30 Connections per second:	6,00,000	Connection per second is very higher side and it is not inline with throughput and Conncurrent connection requirement of Firewall. Due to this clause we are unable to participate in this bid.	Request to change clasue as Connection per second 200K	

Feature	Count for MSLDC Kalwa- 04 Nos.	Count for Corporate Office BKC- 02 Nos.	Count for ALDC Ambazari Nagpur- 04 Nos.	Unit	RAM
Threat Prevention (Minimum)	2.5 Gbps	2.5 Gbps	1 Gbps	GBPS	RAM requirement should be minimum 16 GB RAM or more
NGFW Firewall Throughput (Minimum)	4.5	4.5	2	GBPS	
Connections per second (Minimum)	30K	30K	15K	Connection per second	
Concurrent Sessions (Minimum)	8 Million	8 Million	8 Million	Concurrent sessions	
VPN Throughput (Minimum)	2 Gbps	2 Gbps	1.5 Gbps	GBPS	

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL							
Sr. No.	Vendor	No.	Page No., Clause No.	Description	Vendor		MSETCL
					Querry/Clarification	Changes Required	Revisions & Comments
6	Check point	6.5.2 Firewall Specifications	Page No-25 Clause No 4	The appliance should support at least 12 * 1G Gigabit ports, minimum 2 x 10G SFP+ loaded with multimode module from day 1 and should be scalable to additional 8 * 10G in future	Additonal 8x10G port requirement is providing undue advantage to single OEM hence request to amend	Request to change clause as "The appliance should support at least 8 * 1G Gigabit ports, minimum 2 x 10G SFP+ loaded with multimode module from day 1 and should be scalable to additional 2* 10G in future"	**Revised Clause:** The appliance should support at least 8* 1G Gigabit ports, minimum 2 x 10G SFP+ loaded with multimode module from day 1 and should be scalable to additional 2 * 10G in future

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	No.	Page No., Clause No.	Description	Vendor		MSETCL
					Querry/Clarification	Changes Required	Revisions & Comments
7	Check point	6.5.2 Firewall Specifications	Page No-32 Clause No 4	Should support more than 25,000 (excluding custom signatures) IPS signatures or more. Should support capability to configure correlation rule where multiple rules/events can be combined together for better efficacy	25000 IPS signatures is supported by only single OEM and it is restricting us to participate	Request to change clasue as "Should support more than 12,000 (excluding custom signatures) IPS signatures or more. Should support capability to configure correlation rule where multiple rules/events can be combined together for better efficacy"	**Revised Clause:** The firewall must detect & prevent minimum 12,000 + CVE exploit (exclusing custom signatures) attempts to safeguard Maha Transco environment. OEM to provide full list of IPS signatures a the time of bidding/implementation along with CVE numbers.

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Section	Page Numb	Point	Original Content in RFQ	Vendor		MSETCL
						Change Request	Justification	Revisions and Comments
1	Cisco	Annexure B- Scope of Work (SoW) B. Anti-APT	14	4	Proposed Anti-APT solution will be configured with customized sandbox images as per endpoint and server landscape replicating OS and application environment.	Proposed Anti-APT solution will be configured with customized sandbox images.	Justification: The clause restricts participation, hence request for change.	**Revised Clause:** Proposed Anti-APT solution will be configured with sandbox images
2	Cisco	Annexure B- Scope of Work (SoW) B. Anti-APT	14	11	Provide incident management workflow and process as per best practices with respected to solution provided.	Please Remove	Ideally Incident Response is best done by the Services vendor who is managing SOC as it involves co-ordination between multiple security products deployed in SOC. Hence this services cannot be under the scope of just the APT vendor.	**Revised Clause:** Provide incident management integration capability with SOAR/SIEM etc. as per best practices with respected to solution provided.

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Section	Page Numb	Point	Original Content in RFQ	Vendor		MSETCL
						Change Request	Justification	Revisions and Comments
3	Cisco	Annexure B-Scope of Work (SoW) B. Anti-APT	15	20	Solution shall monitor, detect, alert, report and provide remediation, recommendation for infections discovered using SPAN or mirror traffic.	Solution shall monitor, detect, alert, report and provide recommendation for infections discovered using SPAN or mirror traffic.	Justification: Providing remediation is not possible as the appliance will not be inline to take action.	**Revised Clause:** Solution shall monitor, detect, alert, report and provide recommendation for infections discovered using SPAN or mirror traffic.
4	Cisco	Annexure A-Technical Specifications: Anti-APT solution Specifications	19	1	The Anti-APT solution offered must be rated as ‘leaders’ or 'Challengers' in the Gartner Magic Quadrant published by Gartner from last three years.	The Anti-APT solution offered must be rated as ‘leaders’ or 'Challengers' in the Gartner Magic Quadrant published by Gartner from last three years or Must be rated as "Top Players" in the Radicati APT production market quadrant published by Radicati in any one of the last three years	Gartner Magic Quadrant Anti- apt is not published any more. Request to allow Radicati report too	**Revised Clause:** The Anti-APT solution offered must be rated as Top Player or specialist in Redicati APT production quadrant published by Redicati in any of last 3 years or Anti-APT solution operating system must be NIAP (National Information Assurance Partnership) Common Criteria certified.

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Section	Page Numb	Point	Original Content in RFQ	Vendor		MSETCL
						Change Request	Justification	Revisions and Comments
5	Cisco	Annexure A-Technical Specifications: Anti-APT solution Specifications	20	13	Solution should track the infection or threat history for a device with the ability to access all forensic evidence for past infections (9 months)	Solution should track the infection or threat history for a device with the ability to access all forensic evidence for past infections.	Justification. For longer retention of data for forensic integration with syslog can be used	**Revised Clause:** Solution should track the infection or threat history for a device with the ability to access all forensic evidence for past infections.
6	Cisco	Annexure A-Technical Specifications: Anti-APT solution Specifications	20	20	Inspect Proxy, DNS, http, https traffic	Solution shall have capability to analyze and block TCP/UDP protocol to identify attacks and malware communications. At minimum, the following protocols are supported for real-time inspection, blocking and control of download files: HTTP, SMTP, POP3, IMAP, NetBIOS-SSN and FTP	Justification: For inspection of DNS traffic, DNS security solution is needed	**Revised Clause:** Inspect Proxy, http, https traffic

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Section	Page Numb	Point	Original Content in RFQ	Vendor		MSETCL
						Change Request	Justification	Revisions and Comments
7	Cisco	Annexure A- Technical Specifications: Anti-APT solution Specifications	21	29	Solution should be capable to integrate with devices link Enterprise Antivirus product to mitigate risk by blocking similar threat by pushing hashes/signature.	Please remove.	Justification: Most of the OEM will not be able to provide as this clause requires AV and Anti-apt to be given by same vendor	**To be Removed**

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Section	Page Number	Point	Original Content in RFQ	Vendor		MSETCL
						Change Request	Justification	Revisions and Comments
1	Cisco	Annexure B- Scope of Work (SoW) B. Antivirus and EDR	16	2	The solution must support integration to Active Directory	Please Remove		No Change
2	Cisco	Annexure A- Technical Specifications : EDR Specifications	26	11	The Solution Shall have feature to set scan priority on the host to prevent performance degradation.	The Solution Shall have feature to set/schdule scan on the host to prevent performance degradation.	Justification: different OEM use different approach	**Revised Clause:** The Solution Shall have feature to set/**schedule** scan on the host to prevent performance degradation.
3	Cisco	Annexure A- Technical Specifications : EDR Specifications	26	12	The Solution Shall be able to monitor and deliver suspicious activity detection like Activity Scoring and Anomaly Detection, Rule-Based Detection, Threat Intelligence-Based Detections.	The Solution Shall be able to monitor and deliver suspicious activity detection like Anomaly Detection, Rule-Based Detection, Threat Intelligence-Based Detections.		**Revised Clause:** The Solution Shall be able to monitor and deliver suspicious activity detection like Activity Scoring/Anomaly Detection/Rule-Based Detection/Threat Intelligence- Based Detections IOC rules.

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Section	Page Number	Point	Original Content in RFQ	Vendor		MSETCL
						Change Request	Justification	Revisions and Comments
4	Cisco	Annexure A-Technical Specifications : EDR Specifications	27	16	The Solution must be able to provide a detailed report of individual client and must consist of following information, not limited to: Hostname and Mac address, DNS config, Last scan status, any pending scan request, IP address, Username logged in, Agent installed date.	The Solution must be able to provide a detailed report of individual client and must consist of following information, not limited to: Hostname Last scan status, any pending scan request, IP address, Agent installed date.		**Revised Clause:** The Solution must be able to provide a detailed report of individual client and must consist of following information, not limited to: **Hostname/Mac address/DNS config**, Last scan status, any pending scan request, IP address, Username logged in, Agent installed date.

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL								
Sr. No.	Vendor	Section	Page Number	Point	Original Content in RFQ	Vendor		MSETCL
						Change Request	Justification	Revisions and Comments
5	Cisco	Annexure A-Technical Specifications : EDR Specifications	27	17	The Solution must support detection of hooking methods like, but not limited to: SSDT hooks, Alternate SSDT hook (KTHREAD Service Table), IDT hooks (interrupt descriptor table), System drivers IO hooks, System entry (SYSENTER and int2E) hooks, local and global windows hooks (Set Windows HookEx), User mode hooks (IAT, EAT, Inline) for processes and DLL's, Model specific registers hooks, Kernel Object hooks, Metasploit detections.	The Solution must support detection of hooking methods .	Justification: To Protect organisation against unknown and zero-day threats, different OEM use different approach like AV or APT and requesting for specfic set of hooking technique restrict participation hence requesting change.	**Revised Clause:** The Solution must support detection of hooking methods .
6	Cisco	Annexure A-Technical Specifications : EDR Specifications	27	20	The Solution shall allow IP detections. Example If same IP was accessed repeatedly at an interval of 25% of the standard deviation. The Solution shall allow changing the percentages as required.	Please Remove	Justification: Not a unctionality of EDR	**Revised Clause:** Solution shall allow malicious IP Detections

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Section	Page Number	Point	Original Content in RFQ	Vendor		MSETCL
						Change Request	Justification	Revisions and Comments
7	Cisco	Annexure A-Technical Specifications : EDR Specifications	27	21	The Solution shall provide capabilities to have correlation with SIEM and Multi Factor logs and packets to provide comprehensive analysis and investigation capabilities in a single interface.	The Solution shall provide capabilities to have correlation with SIEM to provide comprehensive analysis and investigation capabilities in a single interface.	Justification : EDR logs can be sent to SIEM whether further investigation of the logs can be performed via co-relating logs from multiple sources.	**Revised Clause:** The Solution shall provide capabilities to have correlation with SIEM to provide comprehensive analysis and investigation capabilities.
8	Cisco	Annexure A-Technical Specifications : EDR Specifications	27	24	Shall collect data from systems like: Running processes, loaded libraries, Drivers, Autoruns, Network connections, network shares, logged on user, AV, patches etc	Shall collect data from systems like: Running processes, loaded libraries, Drivers, Autoruns, Network connections, AV, patches etc		**Revised Clause:** Shall collect data from systems like: Running processes/loaded libraries/ Drivers/ Autoruns/ Network connections/ network shares/ logged on user/ AV/ patches etc
9	Cisco	Annexure A-Technical Specifications : EDR Specifications	28	25	Shall support roaming agents by having the capability to collect data using a DMZ/Cloud Interference.	Do you require a purely Cloud managed EDR solution or On premise set up with hybrid capabilities ?		**Clarification:** EDR is an On premise Set Up with hybrid capabilities

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL								
Sr. No.	Vendor	Section	Page Number	Point	Original Content in RFQ	Vendor		MSETCL
						Change Request	Justification	Revisions and Comments
10	Cisco	Annexure A-Technical Specifications : EDR Specifications	28	31	Threat Intelligence based detections Shall support: IP addresses, domains, hashes, certificates etc, provide native threat intel feeds, provides community threat intel feeds, custom/external threat intel, STIX based threat intel, file reputation service to flag blacklisted hashes from multiple AV vendors.	Threat Intelligence based detections Shall support: IP addresses, domains, hashes, etc, provide native threat intel feeds, provides community threat intel feeds, custom/external threat intel, STIX based threat intel, file reputation service to flag blacklisted hashes from multiple AV vendors.		**Revised Clause:** Threat Intelligence based detections Shall support: IP addresses, domains, hashes, etc,
11	Cisco	Annexure A-Technical Specifications : EDR Specifications	28	32	Threat Intelligence based detections Shall support: IP addresses, domains, hashes, certificates etc, provide native threat intel feeds, provides community threat intel feeds, custom/external threat intel, STIX based threat intel, file reputation service to flag blacklisted hashes from multiple AV vendors	Please Remove	Justification :Duplicate point 31	To be removed

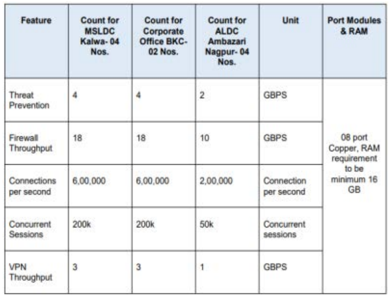
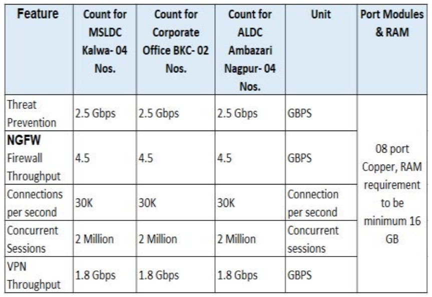
Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Section	Page Number	Point	Original Content in RFQ	Vendor		MSETCL
						Change Request	Justification	Revisions and Comments
12	Cisco	Annexure A-Technical Specifications : EDR Specifications	28	33	Solution Shall support complete digital signatures validation of all executable files	Please Remove		No Change
13	Cisco	Annexure A-Technical Specifications : EDR Specifications	28	35	The Solution shall support capability to pull specific files and entire file system from the endpoint.	The Solution shall support capability to pull specific files from the endpoint.		**Revised Clause:** The Solution shall support capability to pull specific files **or** entire file system from the endpoint.
14	Cisco	Annexure A-Technical Specifications : EDR Specifications	29	37	Support analysis of system not connected to the network and last scan results	Provide last scan results of system when not connected to the network for later analysis		**Revised Clause:** Provide last scan results of system when not connected to the network for later analysis
15	Cisco	Annexure A-Technical Specifications : EDR Specifications	29	41	Shall have option to dump full memory osf a system and process for further analysis.	Please Remove	Justification : memory dump can be performed via system OS	To be removed

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL								
Sr. No.	Vendor	Section	Page Number	Point	Original Content in RFQ	Vendor		MSETCL
						Change Request	Justification	Revisions and Comments
16	Cisco	Annexure A- Technical Specifications : EDR Specifications	29	42	Shall have feature to transfer desired modules to an external sandbox environment for analysis.	Please Remove	Justification : For better efficacy it best that EDR automatically decide which module is looked by which edr engine	No Change
17	Cisco	Annexure A- Technical Specifications : EDR Specifications	29	45	The Solution shall allow remote install/remove of the agents on endpoint machine	Please Remove	Justification : This can be performed via SSCM or GPO deployment tool	No Change
18	Cisco	Annexure A- Technical Specifications : EDR Specifications	29	47	The solution shall be able to change the communication port between the management console and management server	Please Remove		No Change

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Section	Page Number	Point	Original Content in RFQ	Vendor		MSETCL
						Change Request by Vendor	Justifictaion	Revisions and Comments
1	Cisco	Annexure B-Scope of Work (SoW) B. NGFW	10	10	MSETCL is looking to implement Next Generation Firewall (NGF) with an integrated solution of Application Intelligence and Control, IPS, URL filtering, Anti-bot, Anti-virus, Anti-spyware, Web reputation, Identity awareness and VPN (both IPSec and SSL). The firewall would be deployed in the MSLDC, ALDC and BKC in active / active mode. For perimeter firewall (External) and Internal Firewall MSETCL intends to have different make firewall.	MSETCL is looking to implement Next Generation Firewall (NGF) with an integrated solution of Application Intelligence and Control, IPS, URL filtering, **Anti-bot/Anti-virus/Anti-spyware/Anti-malware** Web reputation, Identity awareness and VPN (both IPSec and SSL). The firewall would be deployed in the MSLDC, ALDC and BKC in **active / passive mode.** For perimeter firewall (External) and Internal Firewall MSETCL intends to have different make firewall.	To Protect organisation against unknown and zero-day threats, different OEM use different approach like AV or APT and hence requesting change. The proposed firewall is able to handle the required firewall throughput on a single appliance .A/A is used on firewalls when a single firewall is not able to cater to the throughput requirements of the appliance. This point pushes certain OEM to quote bigger box hence for broader participation requesting to change the clause.	**Revised Clause:** MSETCL is looking to implement Next Generation Firewall (NGF) with an integrated solution of Application Intelligence and Control, IPS, URL filtering, **Anti-bot, Anti-virus, Anti-spyware, Anti-malware**, Web reputation, Identity awareness and VPN (both IPSec and SSL). The firewall would be deployed in the MSLDC, ALDC and BKC in **active/passive or active/active mode (One of the mode has to be operational based on disscussion with MSETCL)**. For perimeter firewall (External) and Internal Firewall MSETCL intends to have different make firewall.
2	Cisco	Annexure B-Scope of Work (SoW) B. NGFW	10	10	Solution should have Incident Response service(in case of any threat/incident)	Please remove.	Ideally Incident Response is best done by the Services vendor who is managing SOC as it involves co-ordination between multiple security products deployed in SOC. Hence this services cannot be under the scope of just the Firewall vendor.	**Revised Clause:** The Solution should have the integration capability with Incident Response System such as SOAR/SIEM etc.
3	Cisco	Annexure B-Scope of Work (SoW) B. NGFW	10	13	Enforce policy and perform threat analysis on all access from presentation servers to application back-end components, middleware and data-sources.	**Clarification:** Unclear point. By access you mean allow or block communication? Also, please specify you are referring to the traffic within the same or different subnet?		**Revised Clause:** Enforce policy and perform threat analysis **within same subnet** on all access from presentation servers to application back-end components, middleware and data-sources.
4	Cisco	Annexure B-Scope of Work (SoW) B. NGFW	11	21	Solution should Reconstruct files with known safe elements to eliminate infected files from entering your network.	Please remove.	Justification: file detected with malware should be quarantine instead of trying to clean the content and forwarding what looks to be clean but it may or may not be. Also by removing all the active content and macros sending only a clean document we are breaking the data integrity.	**No Change**

<table>
<tr><th colspan="9">Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL</th></tr>
<tr><th>Sr. No.</th><th>Vendor</th><th>Section</th><th>Page Number</th><th>Point</th><th>Original Content in RFQ</th><th colspan="2">Vendor</th><th>MSETCL</th></tr>
<tr><th></th><th></th><th></th><th></th><th></th><th></th><th>Change Request by Vendor</th><th>Justifictaion</th><th>Revisions and Comments</th></tr>
<tr><td>5</td><td>Cisco</td><td>Annexure A- Technical Specifications: Firewall Specifications</td><td>30</td><td>6.5.1</td><td>Firewall sizing

<table>
<tr><th>Feature</th><th>Count for MSLDC Kalwa- 04 Nos.</th><th>Count for Corporate Office BKC- 02 Nos.</th><th>Count for ALDC Ambazari Nagpur- 04 Nos.</th><th>Unit</th><th>Port Modules & RAM</th></tr>
<tr><td>Threat Prevention</td><td>4</td><td>4</td><td>2</td><td>GBPS</td><td>08 port Copper, RAM requirement to be minimum 16 GB</td></tr>
<tr><td>Firewall Throughput</td><td>18</td><td>18</td><td>10</td><td>GBPS</td><td></td></tr>
<tr><td>Connections per second</td><td>6,00,000</td><td>6,00,000</td><td>2,00,000</td><td>Connection per second</td><td></td></tr>
<tr><td>Concurrent Sessions</td><td>200k</td><td>200k</td><td>50k</td><td>Concurrent sessions</td><td></td></tr>
<tr><td>VPN Throughput</td><td>3</td><td>3</td><td>1</td><td>GBPS</td><td></td></tr>
</table></td><td>Firewall Sizing

<table>
<tr><th>Feature</th><th>Count for MSLDC Kalwa- 04 Nos.</th><th>Count for Corporate Office BKC- 02 Nos.</th><th>Count for ALDC Ambazari Nagpur- 04 Nos.</th><th>Unit</th><th>Port Modules & RAM</th></tr>
<tr><td>Threat Prevention</td><td>2.5 Gbps</td><td>2.5 Gbps</td><td>2.5 Gbps</td><td>GBPS</td><td>08 port Copper, RAM requirement to be minimum 16 GB</td></tr>
<tr><td><b>NGFW</b> Firewall Throughput</td><td>4.5</td><td>4.5</td><td>4.5</td><td>GBPS</td><td></td></tr>
<tr><td>Connections per second</td><td>30K</td><td>30K</td><td>30K</td><td>Connection per second</td><td></td></tr>
<tr><td>Concurrent Sessions</td><td>2 Million</td><td>2 Million</td><td>2 Million</td><td>Concurrent sessions</td><td></td></tr>
<tr><td>VPN Throughput</td><td>1.8 Gbps</td><td>1.8 Gbps</td><td>1.8 Gbps</td><td>GBPS</td><td></td></tr>
</table></td><td>Justification: The threat prevention througput can't 90% of the NGFW througput as enabling anti-apt check on the appliance result a throughput degradation of nearly 40-50%.
The connection/sec can't be greater than maxmium connection of the appliance.
As the RFP is for NGFW firewall requesting to consider NGFW throughput not just Firewall(stateful) throughput for sizing.</td><td>Revised Clause:
<table>
<tr><th>Feature</th><th>Count for MSLDC Kalwa- 04 Nos.</th><th>Count for Corporate Office BKC- 02 Nos.</th><th>Count for ALDC Ambazari Nagpur- 04 Nos.</th><th>Unit</th><th>RAM</th></tr>
<tr><td>Threat Prevention (Minimum)</td><td>2.5 Gbps</td><td>2.5 Gbps</td><td>1 Gbps</td><td>GBPS</td><td>RAM requirement should be minimum 16 GB RAM or more</td></tr>
<tr><td><b>NGFW</b> Firewall Throughput (Minimum)</td><td>4.5</td><td>4.5</td><td>2</td><td>GBPS</td><td></td></tr>
<tr><td>Connections per second (Minimum)</td><td>30K</td><td>30K</td><td>15K</td><td>Connection per second</td><td></td></tr>
<tr><td>Concurrent Sessions (Minimum)</td><td>8 Million</td><td>8 Million</td><td>8 Million</td><td>Concurrent sessions</td><td></td></tr>
<tr><td>VPN Throughput (Minimum)</td><td>2 Gbps</td><td>2 Gbps</td><td>1.5 Gbps</td><td>GBPS</td><td></td></tr>
</table></td></tr>
<tr><td>6</td><td>Cisco</td><td>Annexure A- Technical Specifications: Firewall Specifications</td><td>33</td><td>25</td><td>The proposed Firewall shall be able to scan & find for unknown threats in executable, archive files, documents, JAVA and flash specifically: 7z, cab, csv, doc, pdf, potx, pps, ppsm, ppsx, ppt, pptm, pptx, rar, rtf, scr, swf, tar tgz, docm, docx, dot, dotm, dotx, jar, xla, xls, xlsb, xlsm, xlsx, xlt, xltm, xltx, xlw, zip etc</td><td>The proposed Firewall shall be able to scan & find for unknown threats in executable, archive files, documents, JAVA and flash specifically: <b>7z, cab, doc, pdf, , ppt, , pptx, rar, rtf, scr, swf, tar, docx, jar, xls, xlsx, xlw, zip etc</b>.</td><td>Justification: To Protect organisation against unknown and zero-day threats, different OEM use different approach like AV or APT and requesting for specfic set of file type restrict participation hence requesting change.</td><td>No Change</td></tr>
<tr><td>7</td><td>Cisco</td><td>Annexure A- Technical Specifications: Firewall Specifications</td><td>33</td><td>29</td><td>NG Firewall should support Active/Standby failover and Active/Active</td><td>NG Firewall should support <b>Active/Standby</b> failover.</td><td>Justification: The proposed firewall is able to handle the required firewall throughput on a single appliance .A/A is used on firewalls when a single firewall is not able to cater to the throughput requirements of the appliance. This point push Certain OEM to quote bigger box hence for broader participation requesting to change the clause.</td><td>NG Firewall should support Active/Standby failover <b>OR</b> Active/Active <b>(One of the mode has to be operational based on disscussion with MSETCL)</b></td></tr>
</table>

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Section	Page Number	Point	Original Content in RFQ	Vendor		MSETCL
						Change Request by Vendor	Justifictaion	Revisions and Comments
8	Cisco	Annexure A-Technical Specifications: Firewall Specifications	34	45	The NGFW MUST provide reports on Latency, Jitter & Packet loss on the links of Individual Link Quality/Virtual Link Quality on daily, weekly, monthly etc.	Please remove	Justification: The requested features are functionality of a SD-wan or Wan optimization solution, not the feature of firewall.	The NGFW **may preferably** provide reports on Latency, Jitter & Packet loss on the links of Individual Link Quality/Virtual Link Quality on daily, weekly, monthly etc.
9	Cisco	Annexure A-Technical Specifications: Firewall Specifications	35	49	The NBA capability must provide the option of supplying end point intelligence to the IPS for correlation against intrusion events to aid in event impact prioritization	The firewall should have capability to provide the option of supplying end point intelligence to the IPS for correlation against intrusion events to aid in event impact prioritization.	Justification: The requested feature is supported but as firewall capability & not as NBA feature, hence requesting to change the language of the clause.	The **Firewall** capability must provide the option of supplying end point intelligence to the IPS for correlation against intrusion events to aid in event impact prioritization.
10	Cisco	Annexure A-Technical Specifications: Firewall Specifications	35	50	Solution should have Incident Response service (in case of any threat/incident)	Please remove.	Ideally Incident Response is best done by the Services vendor who is managing SOC as it involves co-ordination between multiple security products deployed in SOC. Hence this services cannot be under the scope of just the Firewall vendor.	**Revised Clause:** The Solution should have the integration capability with Incident Response System such as SOAR/SIEM etc.
11	Cisco	Annexure A-Technical Specifications: Firewall Specifications	35	51	Provide the capability to monitor and report on configuration of the solution controls in respect to compliance with standards (ISO27001, PCI-DSS, NERC-CIP etc)	Provide the capability to monitor and report on configuration of the solution controls in respect to compliance with standards.	Justification: Different OEM have different pre-built template for monitoring and reporting purpose. Hence requesting change for broader participation.	**Revised Clause:** Provide the capability to monitor and report on configuration of the solution controls in respect to compliance with standards.

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Section	Page Number	Point	Original Content in RFQ	Vendor		MSETCL
						Change Request by Vendor	Justifictaion	Revisions and Comments
12	Cisco	Annexure A-Technical Specifications: Firewall Specifications	35	54	The solution should have provision to provide VPN access through multi factor authentication & support Multi factor authentication methods listed below, a. Active Directory b. LDAP c. RADIOUS d. SMS based OTP e. Email based OTP, etc	The solution should have provision to provide VPN access **through integration with Multi factor authentication methods/solution** listed below, a. Active Directory b. LDAP c. RADIUS d. SMS based OTP	Justification: having in-built MFA restricts participation , hence requesting to change the clause for broader participation.	**Revised Clause:** The solution should have provision to provide VPN access **through integration with Multi factor authentication methods/solution** listed below, a. Active Directory b. LDAP c. RADIUS d. **SMS/Email** based OTP
13	Cisco	Annexure A-Technical Specifications: Firewall Specifications	35	55	The solution should have provision for blocking the traffic based on YARA Rule	The solution should have provision for blocking the traffic based on **YARA Rule/SHA-256 /MD5 hash/AV signature** to detect malware.	Justification: To Protect organisation against unknown and zero-day threats, different OEM use different approach, Hence request to allow a host of options as suggested above	**Revised Clause:** The solution should have provision for blocking the traffic based on **YARA Rule/SHA-256 /MD5 hash/AV signature** to detect malware.

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No	Vendor	Page No	Clause	RFP Clause	Vendor	MSETCL
					Modification Required	Revisions & Comments
1	Fortinet	30	Firewall Sizing	08 port Copper, RAM requirement to be minimum 16 GB	Fortigate Solution has ability to deliver higher performance with low memory.we strongly belive adopting superior technology not only enables to deliver higher throughput utilizing low resource, but also reduce carbon footprint. Also typically Firewall sizing is to be done on the Throughput, Concurrent connections, session per seconds. RAM is not the sizing parameter for the firewall sizing. Hence please remove the RAM requirement clause from the RFP.	RAM Required to be minimum 16GB or higher
2	Fortinet	31	Firewall Specification	The appliance should support at least 12 * 1G Gigabit ports, minimum 2 x 10G SFP+ loaded with multimode module from day 1 and should be scalable to additional 8 * 10G in future	1) This clause is not matching the port requirement mention on page 30 Firewall sizing, hence kindly claify the same 2) Why do we need additional 8 x 10G ports considering the throughput requirement is 4 Gbps and 2 Gbps, as the 10G ports would be cosmetic in nature ?	**Revised Clause:** **The appliance should support at least 8* 1G Gigabit ports, minimum 2 x 10G SFP+ loaded with multimode module from day 1 and should be scalable to additional 2 * 10G in future**

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No	Vendor	Page No	Clause	RFP Clause	Vendor	MSETCL
					Modification Required	Revisions & Comments
3	Fortinet	31	Firewall Specification	Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats. The appliance hardware should be a multicore CPU architecture with a hardened 64-bit operating system to support higher memory	Fortinet is in the Gartner Leaders Quadrant for last one decade with top Govermenet, Telecom and BFSI customers. This clause will not let Fortinet participate in the bid and no where it helps MSETECL in terms of technology or features. Infact it restricts MSETCL to not explore a world class proven product for their critical requirement. We request MSTECL to please remove this clause.	**To be Removed**
4	Fortinet	31	Firewall Specification	The proposed solution should have dual redundant power supply and redundant hot swappable fans.	The Firewall generally have in-built redundant FANs to ensure that the internal components are provided sufficient cooling and resiliency to failure. The replaceable/Swappable without reloading device clause is more towards specific OEMs and does not give any additional benefit from a hardware standpoint. Request you to modify the clause as " The proposed solution should have dual redundant power supply and redundant fans.	**Revised Clause:** The proposed solution should have dual redundant power supply and redundant fans.

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No	Vendor	Page No	Clause	RFP Clause	Vendor	MSETCL
					Modification Required	Revisions & Comments
5	Fortinet	32	Firewall Specification	Should support more than 25,000 (excluding custom signatures) IPS signatures or more. Should support capability to configure correlation rule where multiple rules/events can be combined together for better efficacy	IPS Signatures vary from one OEM to another, and never the right benchmark to arrive at a minimum number. hence Kindly modify this clause as "Should support more than 20,000+ (excluding custom signatures) IPS signatures or more. Should support capability to configure correlation rule where multiple rules/events can be combined together for better efficacy"	**Revised Clause:** The firewall must detect & prevent minimum 12,000 + CVE exploit (excluding custom signatures) attempts to safeguard Maha Transco environment. OEM to provide full list of IPS signatures at the time of bidding/implementation along with CVE numbers.
6	Fortinet	35	Firewall Specification	The solution must provide a full-featured NBA capability to detect threats emerging from inside the network (i.e., ones that have not passed through a perimeter IPS). This includes the ability to establish “normal” traffic baselines through flow analysis techniques (e.g., NetFlow) and the ability to detect deviations from normal baselines.	This is not the function of the NGFW hence request you to remove this clause.	The solution **may preferably** provide **integration with** full-featured NBA capability to detect threats emerging from inside the network (i.e., ones that have not passed through a perimeter IPS). This includes the ability to establish “normal” traffic baselines through flow analysis techniques (e.g., NetFlow) and the ability to detect deviations from normal baselines.

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL						
Sr. No	Vendor	Page No	Clause	RFP Clause	Vendor	MSETCL
					Modification Required	Revisions & Comments
7	Fortinet	36	Firewall Specification	The NBA capability must provide the option of supplying end point intelligence to the IPS for correlation against intrusion events to aid in event impact prioritization.	This is not the function of the NGFW hence request you to remove this clause.	The **Firewall** capability must provide the option of supplying end point intelligence to the IPS for correlation against intrusion events to aid in event impact prioritization.
8	Fortinet	35	Firewall Specification	Provide the capability to monitor and report on configuration of the solution controls in respect to compliance with standards (ISO27001, PCI-DSS, NERC-CIP etc.).	This is not the core function of the next generation firewall, and would required additional third party components that needs to be factor as part of the solution. hence kindly clarify	**Revised Clause:** Provide the capability to monitor and report on configuration of the solution controls.
9	Fortinet	19	Anti-APT solution specifications	The Anti-APT solution offered must be rated as 'leaders' or 'Challengers' in the Gartner Magic Quadrant published by Gartner from last three years.	There is no quadrant for the Anti-APT solution , so kindly validate the same and request to remove this clause.	**Revised Clause:** The Anti-APT solution offered must be rated as Top Player or specialist in Redicati APT production quadrant published by Redicati in any of last 3 years or Anti-APT solution operating system must be NIAP (National Information Assurance Partnership) Common Criteria certified.

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No	Vendor	Page No	Clause	RFP Clause	Vendor	MSETCL
					Modification Required	Revisions & Comments
10	Fortinet	19	Anti-APT solution specifications	Inspect UDP traffic	UDP protocol used for the voice and there are no files transmitted over the UDP protocol, hence request to remove this clause	**Revised Clause:** May Inspect UDP Traffic
11	Fortinet	20	Anti-APT solution specifications	Solution should support both inline and out of the band mode	All Anti-APT solutions are place in out of the band mode. Only one vendor support inline mode deployment, and hence request to modify this clause as " Solution should suppor out of the band mode deployment, standalone mode or integration with the Firewall"	**Revised Clause:** Solution should support out of the band mode deployment, standalone mode or integration with the Firewall
12	Fortinet	20	Anti-APT solution specifications	Inspect Proxy, DNS, http, https traffic	DNS protocol used for the domain resolution and it dosent carry any files and hence dns is not relavent to the Anti-APT. so kindly modify this clause as "inspect Proxy, http nad https traffic"	**Revised Clause:** Inspect Proxy, http, https traffic
13	Fortinet	36	Antivirus Specification	The Antivirus solution offered must be rated as 'leaders' or 'Challengers' in the Gartner Magic Quadrant published by Gartner from last three years.	Kindly remove this clause so other OEM can also participate in the RFP	The Antivirus solution offered must be rated as 'leaders' or 'Challengers' in the Gartner Magic Quadrant for endpoint protection platform published by Gartner in atleast any one of the last three years.
14	Fortinet	36	Antivirus Specification	The Central Management Solution should have capabilities to manage the Servers at Primary site & DR Site	Can you please elaborate this clause, what is manage servers ?	Manage Servers refers to managing the both the server locations centrally.

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No	Vendor	Page No	Clause	RFP Clause	Vendor	MSETCL
					Modification Required	Revisions & Comments
15	Fortinet	37	Antivirus Specification	Solution should protect the data transfer from endpoints to the hacker system spoofed IP or MAC address. (Anti IP and MAC spoofing).	This clause is belongs to network level firewall/Gateway and hence request you to remove this clause.	**Revised Clause:** Solution should protect the data exfiltration/transfer from endpoints.
16	Fortinet	37	Antivirus Specification	Solution should scan, detect, clean or delete malicious code software for protocols POP3, POP3S, SMTP, and SMTPS	This clause is belongs to network level firewall/gateway and hence request you to remove this clause.	**Revised Clause:** Solution should scan, detect, clean or delete malicious code software for protocols SMTP/SMTPS.
17	Fortinet	37	Antivirus Specification	Solution should allow creating and deploying user defined firewall policy for endpoints to permit or deny network access based over IP Address, logical Ports, and Services on a single IP Address, range, and segments	This clause is belongs to network level firewall/gateway and hence request you to remove this clause.	To be removed
18	Fortinet	38	Antivirus Specification	Solution should provide a Utility Software Tool for all variant other than Windows Operating System for collecting infected endpoints log for analysing and developing signatures which can clean the endpoints from Malware infection.	Which all all Non-windows OS is expected, need better clarity	Linux (ESXI, Ubuntu, Red Hat) & Solaris 10

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No	Vendor	Page No	Clause	RFP Clause	Vendor	MSETCL
					Modification Required	Revisions & Comments
19	Fortinet	25	EDR Sizing	Events per day 1500000	Typically EDR sizing is done on the number of endpoints and not the Events per day or seconds, hence request to modify this clause and mention the how many endpoints	Events per day to be removed.
20	Fortinet	25	EDR Specifications	The EDR solution offered must be rated as 'leaders' or 'Challengers' in the Gartner Magic Quadrant published by Gartner from last three years.	Kindly remove this clause so other OEM can also participate in the RFP	**Revised Clause:** The EDR solution offered must have detection rate of more than 80% or more as per MITRE Engenuity ATT&CK® Evaluations published by MITRE 2022 or Should be listed as 'Leaders' or 'Strong Performers' in The Forrester Wave Report in atleast any one of the last three years as published by Forrester Research Inc.
21	Fortinet	26	EDR Specifications	The Solution must support remote clean-up of infected clients through integration with third party Solutions.	Needs more explanation and an example of such 3rd party solution. Custom scripts are supported and they can be utilized to trigger any 3rd party solution	**Clarification:** Custom Scripts will be accepted for triggering any third party solution
22	Fortinet	26	EDR Specifications	The Solution must do baseline scans of hosts and use this information to build a database of all unique files for comparison with future scans.	Since our EDR need not to scan the file and it idenify the threat based on the telemetry data of the file activites this is not appliacble, hence request to remove this clause	**No Change**

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No	Vendor	Page No	Clause	RFP Clause	Vendor	MSETCL
					Modification Required	Revisions & Comments
23	Fortinet	26	EDR Specifications	The Solution Shall have feature to set scan priority on the host to prevent performance degradation.	We do scan but it is an scheduled scan only. Since our EDR need not to scan the file and it idenify the threat based on the telemetry data of the file activites. Or you can change to The Solution must be able to set the periodic scan for group of. hosts to set the scan in non peak hours.	**Revised Clause:** The Solution Shall have feature to set/**schedule** scan on the host to prevent performance degradation.
24	Fortinet	27	EDR Specifications	The Solution must support detection of hooking methods like, but not limited to: SSDT hooks, Alternate SSDT hook (KTHREAD Service Table), IDT hooks (interrupt descriptor table), System drivers IO hooks, System entry (SYSENTER and int2E) hooks, local and global windows hooks (Set Windows HookEx), User mode hooks (IAT, EAT, Inline) for processes and DLL's, Model specific registers hooks, Kernel Object hooks, Metasploit detections.	most listed hooks were relevant 10 years ago under rootkit context, today with hyperv and patchguard these are not relevant, hence request to remove this clause	**Revised Clause:** The Solution must support detection of hooking methods .

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL						
Sr. No	Vendor	Page No	Clause	RFP Clause	Vendor	MSETCL
					Modification Required	Revisions & Comments
25	Fortinet	29	EDR Specifications	Shall have feature to perform Static analysis of file by manual upload	This is a feature of sandbox and not the EDR, hence request to remove this clause from the RFP	**Revised Clause:** Should have feature to perform Static analysis of file by manual upload using external sandbox provided by the OEM.
26	Fortinet	30	EDR Specifications	The Solution shall not support CPU Throttling of Agents.	Our solution is one of the lightest on the market with dedicated up-to 1% CPU utilization and 60MB or RAM utilisation in the normal operation. In the Autonomous mode of operation (no access to Core element) the utilisation is slightly increased but with no major impact on the endpoint performance. , hence request to remove this clause.	The Solution shall support CPU Throttling of Agents upto 2% of CPU utilisation.
27	Fortinet	31	SIEM Specifications	The SIEM solution offered must be rated as 'leaders' or 'Challengers' in the Gartner Magic Quadrant published by Gartner from last three years.	Kindly remove this clause so other OEM can also participate in the RFP	**Revised Clause:** The SIEM solution offered must be rated as 'leaders' or 'Challengers' in the Gartner Magic Quadrant published by Gartner **atleast in any one of** the last three years.

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr No	Vendor	Page no	Technical Complaince	Yes/ No	Vendor	MSETCL
					Remarks	Revisions/Comments
1	Kaspersky	Page 14 of 27 D. Anti-APT				
2	Kaspersky	4	Proposed Anti-APT solution will be configured with customized sandbox images as per endpoint and server landscape replicating OS and application		The point is vendor specific . Please modify to points to Proposed Anti-APT solution will be configured with sandbox images	**Revised Clause:** Proposed Anti-APT solution will be configured with sandbox images
3	Kaspersky	9	The solution should have an ability to block malware downloads over different protocols		The point is vendor specific . Please remove the point	**Revised Clause:** Solution shall have capability to analyze and block TCP/UDP protocol to identify attacks and malware communications. At minimum, the following protocols are supported for real-time inspection, blocking and control of download files: HTTP, SMTP, POP3, IMAP, NetBIOS-SSN and FTP
4	Kaspersky	8	The proposed Anti-APT solution should be seamlessly integrated with the SIEM solution, Firewall, and any other existing or future solutions, as required by the MSETCL		Please remove Firewall as this specs is very vendor specific , The point should be mentioned as The proposed Anti-APT solution should be seamlessly integrated with the SIEM solution and or Firewall, and any other existing or future solutions, as required by the MSETCL	No Change

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr No	Vendor	Page no	Technical Complaince	Yes/ No	Vendor	MSETCL
					Remarks	Revisions/Comments
5	Kaspersky	38	APT hardware provided must have integration with NGFW appliance to detect multi stage attacks the solution should include static analysis technologies like IPS, antivirus, antimalware /anti bot, application awareness, URL Filtering and advanced threats through the APT appliance.		Please remove this point as this is vendor specific	No Change
6	Kaspersky	27	Solution shall support role-based administration such as Administrator, Malware Analyst, Database Reader, and Read-only access users.		The point is vendor specific Please modify the point as Solution shall support role-based administration	**Revised Clause:** Solution shall support role-based administration such as Administrator/ Malware Analyst/Database Reader/ Read-only access users.
7	Kaspersky	32	Solution should have capabilities to configure files, IP, URLs and Domains to Black list or whitelist.		Please remove this point as this is vendor specific	**No Change**
8	Kaspersky	Page 14 of 27 E:Antivirus and EDR (Endpoint Detection and Response):				

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr No	Vendor	Page no	Technical Complaince	Yes/No	Vendor	MSETCL
					Remarks	Revisions/Comments
9	Kaspersky	10	The endpoint protection solution (antivirus and EDR) should support all the operating systems (both 32 and 64 bit architecture) that are deployed within MSETCL. This will include Server, endpoints and desktops version of Windows operating systems and the newer version which are rolled out/ would be rolled out during the contract period, all flavors of Linux OS, guest OS in VMs (Using any hypervisor like VMware/ Hyper V/ Citrix etc.) on Windows, UNIX & Linux OS. Solution should support Virtual Desktop. It must support Intel and AMD CPUs both x86 and x64 architecture.		Support for Unix will limit no of vendors can particpate in the RFP . Please modify the point to The endpoint protection solution (antivirus and EDR) should support all the operating systems (both 32 and 64 bit architecture) that are deployed within MSETCL. This will include Server, endpoints and desktops version of Windows operating systems and the newerversion which are rolled out/ would be rolled out during the contract period,, all flavors of Linux OS, guest OS in VMs (Using any hypervisor like VMware/ Hyper V/ Citrix etc.) on Windows,& Linux OS. Solution should support Virtual Desktop. It must support Intel and AMD CPUs both x86 and x64 architecture.	**No Change**

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr No	Vendor	Page no	Technical Complaince	Yes/ No	Vendor	MSETCL
					Remarks	Revisions/Comments
10	Kaspersky	Additional points to be considered for Endpoint antivirus	Should have critical components for total security on the endpoint in single agent. (Antivirus, Antimalware, Vulnerability protection, HIPS, Firewall, Application, web, Device control, encryption & Virtual Patching.Solution should have the capability to provide the full disk encryption, file & folder encryption and removable media encryption and should be able to manage from central management console.Solution should have categories based (like: Adult , gambling, weapons etc.) web control and should be able to filter HTTPS traffic as well.The proposed solution should allow specified user/administrator to obtain remote access to the desktop of a client device through a Network Agent installed on the device. Remote connection to a device through the Network Agent should also possible if the TCP and UDP ports of the client device are closed.		The following points will provide Hardening functionality which will help to reduce the cyber attack surface.	

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Dcoument name	Page No.	Section No.	Clause No.	Actual Clause in the Tender/RFP	Vendor	MSETCL
							Clarification Sought / Amendment Requested	Revisions and Comments
1	L&T	Annexure A-Technical Specifications for SOC Solution	5	Technical Qualifying Requirement	2 (Table point-3)	The Bidder should have ***experience of successful completion of similar works*** in Central Government/State Government/Public Sector Undertaking/Semi Government organizations in India during the last 05 financial years.The cost for the work order/s should be as below: a) at least 1 work order amounting 80% of estimate cost or b)at least 2 work orders each amounting 60% of estimate cost or c) at least 3 work orders each amounting 40% of estimate cost. Note: i**. Similar works must include minimum two components out of 6** i.e. NGFW, SIEM, Anti-APT, EDR, WAF & AntiVirus. Out of these two components, **one must be proposed SIEM**. ii***. For experience purpose, amount pertaining to similar nature of works i.e. supply of these licenses & support for these licenses, will only be considered instead of complete work order value. In case the work order does not clearly specify the values, bidder is expected to get letter from the competent authority from Customer.***	Work in Progress project (Similar work) are acceptable as per your below RFP statement : - ii. For experience purpose, amount pertaining to similar nature of works i.e. supply of these licenses & support for these licenses, will only be considered instead of complete work order value. In case the work order does not clearly specify the values, bidder is expected to get letter from the competent authority from Customer) . **Please provide confirmation**	

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Dcoument name	Page No.	Section No.	Clause No.	Actual Clause in the Tender/RFP	Vendor	MSETCL
							Clarification Sought / Amendment Requested	Revisions and Comments
2	L&T	Annexure A-Technical Specifications for SOC Solution	10	SIEM Tool Sizing	6.1.1	Minimum Target Nodes* including 3 locations i.e., MSLDC Kalwa, Corporate Office BKC & ALDC Ambazari Nagpur -**2000**	Please help us to know followings: 1)Maximum Target Node count/projection ? 2) Node classification along with Projected Count #? [AppServer # ,DB system #,Network system # Endpoints]etc.	Kindly bid in accordance to the minimum technical specifications
3	L&T		10	SIEM Specifications	6.1.2	The SIEM solution offered must be rated as 'leaders' or 'Challengers' in the Gartner Magic Quadrant published by Gartner from last three years.	Request to change "The SIEM solution offered must be rated as ***'leaders' or 'Challengers or' Niche player'*** in the Gartner Magic Quadrant published by Gartner from last three years ". It would provide more options and flexibility to select OEMs	**Revised Clause:** The SIEM solution offered must be rated as 'leaders' or 'Challengers' in the Gartner Magic Quadrant published by Gartner **atleast in any one of** the last three years.

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Dcoument name	Page No.	Section No.	Clause No.	Actual Clause in the Tender/RFP	Vendor	MSETCL
							Clarification Sought / Amendment Requested	Revisions and Comments
4	L&T	Annexure A-Technical Specifications for SOC Solution	19	Anti-APT Sizing	6.2.1	Network traffic and mail traffic cannot be received on the same device. **Yes** Communication channel bandwidth - **Over 2 Gbps** The number of remote infrastructures in which traffic needs to be analysed. **Two or more** The capacities of one Sandbox component are insufficient to analyse all objects within acceptable time frames. **-Yes** The bidders can quote either physical or virtual appliance with min infra specs in terms of RAM and cores -**yes**	Request Interpretation/Elaboration of following statements : **Criterion** **Four- or more server scenario** 1) Network traffic and mail traffic cannot be received on the same device. **Yes** 2)The capacities of one Sandbox component are insufficient to analyse all objects within acceptable time frames. -**Yes**	**Revised Clause:** Anti-APT solution must have minimum 10Mbps of thoroughput for Kalwa and BKC Locations and Minimum 5 Mbps for ALDC Ambazari, and scalable upto 500 Mbps for each locations & should have minimum 8 VM

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Dcoument name	Page No.	Section No.	Clause No.	Actual Clause in the Tender/RFP	Vendor	MSETCL
							Clarification Sought / Amendment Requested	Revisions and Comments
5	L&T	Annexure A-Technical Specifications for SOC Solution	19	Anti-APT solution specifications	6.2.2	The Anti-APT solution offered must be rated as ‘leaders’ or 'Challengers' in the Gartner Magic Quadrant published by Gartner from last three years.	Request to change "The Anti-APT solution offered must be rated as ***‘leaders’ or ‘Challengers or' Niche player***’ in the Gartner Magic Quadrant published by Gartner from last three years. It would provide more options and flexibility to select OEMs	**Revised Clause:** The Anti-APT solution offered must be rated as Top Player or specialist in Redicati APT production quadrant published by Redicati in any of last 3 years or Anti-APT solution operating system must be NIAP (National Information Assurance Partnership) Common Criteria certified.

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL								
Sr. No.	Vendor	Dcoument name	Page No.	Section No.	Clause No.	Actual Clause in the Tender/RFP	Vendor	MSETCL
							Clarification Sought / Amendment Requested	Revisions and Comments
6	L&T	Annexure A-Technical Specifications for SOC Solution	22	WAF Solution specifications	6.3.2	The WAF solution offered must be rated as ‘leaders’ or 'Challengers' in the Gartner Magic Quadrant published by Gartner from last three years.	Request to change "The WAF solution offered must be rated as ***‘leaders’ or ‘Challengers or' Niche player***’ in the Gartner Magic Quadrant published by Gartner from last three years. It would provide more options and flexibility to select OEMs	**Revised Clasue:** The WAF solution offered must be rated as ‘leaders’ or 'Challengers' in the Gartner Magic Quadrant published by Gartner in atleast any one of the last three years / The WAF solution offered should be STQC tested

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Dcoument name	Page No.	Section No.	Clause No.	Actual Clause in the Tender/RFP	Vendor	MSETCL
							Clarification Sought / Amendment Requested	Revisions and Comments
7	L&T	Annexure A-Technical Specifications for SOC Solution	25	EDR Specifications	6.4.2	The EDR solution offered must be rated as ‘leaders’ or 'Challengers' in the Gartner Magic Quadrant published by Gartner from last three years.	Request to change "The EDR solution offered must be rated as ***‘leaders’ or ‘Challengers or' Niche playe*** r’ in the Gartner Magic Quadrant published by Gartner from last three years. It would provide more options and flexibility to select OEMs	**Revised Clause:** The EDR solution offered must have detection rate of more than 80% or more as per MITRE Engenuity ATT&CK® Evaluations published by MITRE 2022 or Should be listed as 'Leaders' or 'Strong Performers' in The Forrester Wave Report in atleast any one of the last three years as published by Forrester Research Inc.
8	L&T	Annexure A-Technical Specifications for SOC Solutio	31	Firewall Specifications	6.5.2	The Firewall solution offered must be rated as ‘leaders’ or 'Challengers' in the Gartner Magic Quadrant published by Gartner from last three years.	Request to change "The Firewall solution offered must berated as ‘***leaders’ or ‘Challengers or' Niche player***’ in the Gartner Magic Quadrant published by Gartner from last three years. It would provide more options and flexibility to select OEMs	The Firewall solution offered must be rated as ‘leaders’ or 'Challengers' in the Gartner Magic Quadrant published by Gartner **atleast in any one of the** last three years.

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Dcoument name	Page No.	Section No.	Clause No.	Actual Clause in the Tender/RFP	Vendor	MSETCL
							Clarification Sought / Amendment Requested	Revisions and Comments
9	L&T	Annexure A-Technical Specifications for SOC Solution	36	Antivirus Specification	6.6.1	The Antivius solution offered must be rated as ‘leaders’ or 'Challengers' in the Gartner Magic Quadrant published by Gartner from last three years.	Request to change "The Antivius solution offered must berated as ‘***leaders’ or ‘Challengers or' Niche player*** ’ in the Gartner Magic Quadrant published by Gartner from last three years. It would provide more options and flexibility to select OEMs	The Antivius solution offered must be rated as ‘leaders’ or 'Challengers' in the Gartner Magic Quadrant published by Gartner **atleast in any one** of the last three years.

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Document	Specs	Vendor	MSETCL
				Query	Revisions & Comments
1	Radware	**Document:** Annexure A-Tech Spec 6.3 WAF Solution **Page:** 22: Point 1	The WAF solution offered must be rated as ‘leaders’ or 'Challengers' in the Gartner Magic Quadrant published by Gartner from last three years.	Gartner Magic Quadrant is majorly inclined towards Commercial/Market coverage and less on technology. Other reports like Forrester Wave is inclined towards Technical capabilities to block attacks incase of attacks and deployment/ Market Coverage **Hence request to consider below specs** The WAF solution offered must be rated as ‘leaders’ or 'Challengers' in the Gartner Magic Quadrant/ Forrester Wave published by Gartner from last three years.	**Revised Clasue:** The WAF solution offered must be rated as ‘leaders’ or 'Challengers' in the Gartner Magic Quadrant published by Gartner in atleast any one of the last three years / The WAF solution offered should be STQC tested
2	Radware	**Document:** Annexure A-Tech Spec 6.3 WAF Solution **Page:** 22: Point 6	The solution shall have controls for Anti Web Defacement and provide ability to check the authorized version of the website content	Anti Web Defacement prevention is not possible via WAF appliances since this kind of attacks can be easily done via DNS hijacking alone which WAF Solution cannot detect **Hence request to delete the specs**	**No Change**

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Document	Specs	Vendor	MSETCL
				Query	Revisions & Comments
3	Radware	**Document:** Annexure A-Tech Spec 6.3 WAF Solution **Page:** 24: Point 20	Solution must have anti-bot protection, Brute force protection with session tracking, Data Guard protection for Information leakage protection and advanced detection methods like- TPS (Transaction per Second) and JavaScript, CAPTCHA Challenge and device fingerprinting.	CAPTCHA is old technology to prevent BOTs and can be easily bypassed via automation tools https://dev.to/tngeene/how-to-bypass-captcha-with-2captcha-and-selenium-using-python-1p9c **Hence request to modify the specs to below** Solution must have anti-bot protection, Brute force protection with session tracking, Data Guard protection for Information leakage protection and advanced detection methods like- TPS (Transaction per Second) and JavaScript/ CAPTCHA Challenge and device fingerprinting.	**Revised Clause:** Solution must have anti-bot protection, Brute force protection with session tracking, Data Guard protection for Information leakage protection and advanced detection methods like- TPS (Transaction per Second) and JavaScript/ CAPTCHA Challenge and device fingerprinting.

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Document	Specs	Vendor	MSETCL
				Query	Revisions & Comments
4	Radware	**Document:** Annexure A-Tech Spec 6.3 WAF Solution **Page:** 24: Point 23	The proposed solution must have load balancing for Layer-4 & layer-7, TCP Optimization, H/W compression, caching, SSL offloading capability and must protect against FTP, SMTP, HTTP, HTTPS and Application layer Dos and DDOS attacks including stress-based DOS and Heavy URL attacks and should also support SSL VPN functionality.	Web Application Firewall is meant to handle Web based traffic to inspect and block malicious traffic If a Bad Actor attacks infrastructure via DDoS as attack vector - Datacenter can be easily brought down even before it reaches WAF And DDoS attack vector targets Stateful appliances where Firewall/ WAF/ IPS etc. are all Stateful in nature SSL VPN is altogether different technology and not related to WAF **Hence request to change the specs to below** The proposed solution must have load balancing for Layer-4 & layer-7, TCP Optimization, H/W compression, caching, SSL offloading capability and must protect against HTTP, HTTPS and Application layer Dos and Heavy URL attacks.	**Revised Clause:** The proposed solution must have load balancing for Layer-4 & layer-7, TCP Optimization, H/W compression, caching, SSL offloading capability and must protect against HTTP, HTTPS and Application layer Dos and Heavy URL attacks.

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Document	Specs	Vendor	MSETCL
				Query	Revisions & Comments
5	Radware	**Document:** Annexure A-Tech Spec 6.3 WAF Solution **Page:** 24: Point 24	The solution should be able to encrypt the user credentials in real time i.e., when the user is typing the credentials for the web application in his/her browser for any web application that is behind the application security solution. This feature should be agentless and should not require installation of any kind of software either on client end or on the application end.	Encrypting user Credential solves only one problem i.e. protecting users from Man in The Middle attack which is anyways taken care by SSL encryption Other than that it is of no use, since a bad actor can simple consider Hash as Password and initiate attack bypass **Hence request to delete the specs**	To be removed

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Document	Specs	Vendor	MSETCL
				Query	Revisions & Comments
6	Radware	**Document:** Annexure A- Tech Spec 6.3 WAF Solution **Page:** 24: Point 25	The proposed WAF must have Application layer encryption service to protect credentials and sensitive fields and support encryption of credentials on real time at client/browser level to ensure the protection from credential-based attack.	Encrypting user Credential solves only one problem i.e. protecting users from Man in The Middle attack which is anyways taken care by SSL encryption Other than that it is of no use, since a bad actor can simple consider Hash as Password and initiate attack bypass **Hence request to delete the specs**	No Change
7	Radware	**Document:** Annexure A- Tech Spec 6.3 WAF Solution **Page:** 25: Point 27	The proposed solution must provide protection against attacks designed to abuse the application functionality. the solution must offer visibility into synthetic traffic originated by bots and legit human traffic. SI must design and size the solution for both web and mobile based application using mobile SDK.	To Protect the traffic BOT attacks need additional information for sizing since it's a dedicated technology which needs to be factored How many request per month volume is expected to be protected ? How many applications is supposed to be protected ? Are we ok to connect the solution with Cloud for AI/ML technology to leverage its intelligence to protect from advance BOT	**Clarification:** **How many request per month volume is expected to be protected? -** Assume basis the Asset Inventory **How many applications is supposed to be protected ? -**

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Document	Specs	Vendor	MSETCL
				Query	Revisions & Comments
8	Radware	**Document:** Annexure A-Tech Spec 6.3 WAF Solution **Page:** 25: Point 28	Solution must use AI/ML based algorithms to detect the anomaly in the application behavior and must not reply on old generation signature-based technologies to detect and prevent the sophisticated attacks including gift card cracking, card enumeration, skimming, password spraying, scraping, spambots & synthetic identities	To Protect the traffic BOT attacks need additional information for sizing since it's a dedicated technology which needs to be factored How many request per month volume is expected to be protected ? How many applications is supposed to be protected ? Are we ok to connect the solution with Cloud for AI/ML technology to leverage its intelligence to protect from advance BOT	**Clarification:** **Are we ok to connect the solution with Cloud for AI/ML technology to leverage its intelligence to protect from advance BOT -** No
9		**New Addition**			**New Addition:** Proposed WAF should not be from the same OEM whose firewall is proposed in this RFP

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Page No., Clause No.	Description	Vendor		MSETCL
				Querry/Clarification	Changes Required	Revision & Comments
1	Softcell	**Technical Qualifying Requirement, pg no- 5**	The Bidder should have experience of successful completion of similar works in Central Government/State Government/Public Sector Undertaking/Semi Government organizations in India during the last 05 financial years. The cost for the work order/s should be as below: a) at least 1 work order amounting 80% of estimate cost or b)at least 2 work orders each amounting 60% of estimate cost or c) at least 3 work orders each amounting 40% of estimate cost. Note: i. Similar works must include minimum two components out of 6 i.e. NGFW, SIEM, Anti-APT, EDR, WAF & AntiVirus. Out of these two components, one must be proposed SIEM. ii. For experience purpose, amount pertaining to similar nature of works i.e. supply of these licenses & support for these licenses, will only be considered instead of complete work order value. In case the work order does not clearly specify the values, bidder is expected to get letter from the competent authority from Customer		Request you to consider the reference from BFSI, request you to read clause as- similar works must include any components out of 6 i.e. NGFW, SIEM, Anti-APT, EDR, WAF & AntiVirus.	

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Page No., Clause No.	Description	Vendor		MSETCL
				Querry/Clarification	Changes Required	Revision & Comments
2	Softcell	Payment shedule	For material (Item no. 7-9,), 100% Payment (Contract amount) will be released within 30 days after successful commissioning and acceptance of work and receipt of invoices. For remaining material/services (Item no. 1-6), 60% payment (Contract amount) will be released within 30 days after successful acceptance of work and receipt of invoices. 20% (Contract amount) payment will be released after satisfactory completion of 1st-year from the date of acceptance of material/services. 10% (Contract amount) payment will be released after satisfactory completion of 2nd -year from the date of acceptance of material/services. Remaining 10% (Contract amount) will be released after satisfactory completion of 3rd -year from the date of acceptance of material/service	Payment terms is very challanging nature , as a bidder we will be providing BG which is cost to us, in this case required relaxation in payment terms	For remaining material and Services (item no 1 to 6) 90% will be released within 30 days after sucsessful acceptance , 5 % after second year renewal and 5% after third year renewal (We request you to please add 2nd and 3rd year renewal / Subscription pricing break up in commercial format) OR Request you to provide Commercials Bifurcation in commercial bid format, as 1st license / Supcription , 2n d year subscription / renewal and 3 rd year subscrition / renewal , Implementation /Deployment cost also - Please change Payment terms as per - For 1 st Year - 60% against material delivery , 30 % after installation and 10 % after go to live and acceptance certificate. 2 nd Year renewal/ subscription - against submission of Invoice - Yearly advance 3 rd Year renewal/ subscription - against submission of Invoice - Yearly	

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Page No., Clause No.	Description	Vendor		MSETCL
				Querry/Clarification	Changes Required	Revision & Comments
3	Softcell	Annexure A, 6.1.2 SIEM Specifications, pg. 10	The SIEM solution offered must be rated as ‘leaders’ or ‘Challengers’ in the Gartner Magic Quadrant published by Gartner from last three years.		The SIEM solution offered must be rated as ‘leaders’ or ‘Challengers’ in the Gartner Magic Quadrant published by Gartner in any of the last three years.	The SIEM solution offered must be rated as ‘leaders’ or ‘Challengers’ in the Gartner Magic Quadrant published by Gartner **in any one of the last three years.**
4	Softcell	Annexure A, 6.1.2 SIEM Specifications, pg. 10	The solution must support automated identification and classification for type of assets (i.e., servers, network devices, mail servers, database servers, etc.,)	please clarify if the expectation is post device log itegration the devices can be identfied and classified		Expectations for post log integration with the respective devices/tools.

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Page No., Clause No.	Description	Vendor		MSETCL
				Querry/Clarification	Changes Required	Revision & Comments
5	Softcell	Annexure A, 6.1.2 SIEM Specifications, pg. 15	The solution must display traffic profiles in terms of packet rate/ traffic volume/ protocol. This capability must be available for complete TCP sessions analysis e.g., application traffic, session recreation and visualization. For example, throw alert if any services within the organization is using an unknown protocol to a foreign IP address with which there was never any communication done earlier.	This clause is OEM specific, kindly change as requested.	This is OEM specific request you to modify as "The solution must display traffic profiles in terms of traffic volume/ protocol. This capability must be available for analysis, For example, throw alert if any services within the organization is using an unknown protocol to a foreign IP address with which there was never any communication done earlier."	**Revised Clause:** The solution must display traffic profiles in terms of traffic volume/ protocol. This capability must be available for analysis, For example, throw alert if any services within the organization is using an unknown protocol to a foreign IP address with which there was never any communication done earlier."
6	Softcell	Annexure A, 6.1.2 SIEM Specifications, pg. 15	The solution should be able to collect and store configuration data from various devices and use it for analysis.		Request to modify as "The solution should be able to collect and store configuration changes from various devices and use it for analysis."	**Revised Clause:** The solution should be able to collect and store configuration changes from various devices and use it for analysis.

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Page No., Clause No.	Description	Vendor		MSETCL
				Querry/Clarification	Changes Required	Revision & Comments
7	Softcell	Annexure A, 6.1.2 SIEM Specifications, pg. 17	Indicate additional features supported by proposed SIEM but not mentioned above.	SOAR is an integral part of SOC solution which is not mentioned in specifications, recommend you to involve SOAR specs.	1. SIEM Solution must have native SOAR capabilities and should be from same OEM. 2. SOAR capabilities within SIEM must not require any separate license and with no restriction on number of analysts. In case SOAR is not native or from different OEM, License should be proposed for 20 analysts. 3. SOAR solution must provide MTTR and MTTD reports/dashboards.	**No Change** (Additional Features will vary from OEMs perspective)
8	Softcell	Annexure A, 6.1.2 SIEM Specifications, pg. 17	The solution must leverage both Supervised and Un-supervised Machine learning techniques without signatures	This clause is OEM specific, kindly change as requested.	"The solution must leverage both Supervised/Un-supervised Machine learning techniques without signatures"	**Revised Clause:** The solution must leverage Supervised/Un-supervised Machine learning techniques without signatures.
9	Softcell	Annexure A, 6.1.2 SIEM Specifications, pg. 17	Events should not be dropped if it’s exceeding the EPS limitation for the period of 48hrs.	We recommend that the events should not be dropped at any point in time, kindly change the clause to	"Events should not be dropped/queued till EPS is beyond the hardware capacity"	**Revised Clause:** Events should not be dropped/queued till EPS is beyond the hardware capacity

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Page No., Clause No.	Description	Vendor		MSETCL
				Querry/Clarification	Changes Required	Revision & Comments
10	Softcell	Annexure A, 6.1.2 SIEM Specifications, pg. 17	SIEM should be able to perform Deep packet inspection using NTA and NBAD along with Layer-4 & Layer-7 flow inspection	This is OEM specfic point and restrictive in nature. Kindly delete this point.	NTA & NBAD are not part of SIEM solution. However, these can be asked as a separate requirement.	**Revised Clasue:** SIEM should support Layer-4 & layer-7 Flow Inspection
11	Softcell	Annexure A, 6.1.2 SIEM Specifications, pg. 17	Solution must support MLIDS, Sandboxing futures	This is OEM specfic point and restrictive in nature. Kindly delete this point.	NTA & NBAD are not part of SIEM solution. However, these can be asked as a separate requirement.	**Revised Clause:** SIEM should support integration with Sandbox solution
12	Softcell	Annexure A-Tech Spec, 6.6 Antivirus, 6.6.1 Antivirus Specification Pg.no 36	Solution should scan, detect, clean or delete malicious code software for protocols POP3, POP3S, SMTP, and SMTPS.	This is OEM specfic point and restrictive in nature. Kindly delete this point.	Specification is favoring particular OEM and restritive in nature. Please dilute mention specification as per suggestion to allow our participation. **The clause should read as:** Solution should scan, detect, clean or delete malicious code software for protocols POP3/ POP3S/SMTP/SMTPS.	**Revised Clause:** Solution should scan, detect, clean or delete malicious code software for protocols SMTP/SMTPS.

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Page No., Clause No.	Description	Vendor		MSETCL
				Querry/Clarification	Changes Required	Revision & Comments
13	Softcell	Annexure A-Tech Spec, 6.6 Antivirus, 6.6.1 Antivirus Specification Pg.no 38	Solution should support to block external devices like USB, Data Card, Infrared, and Bluetooth.	This is OEM specfic point and restrictive in nature. Kindly delete this point.	Specification is favoring particular OEM and restritive in nature. Please dilute mention specification as per suggestion to allow our participation. **The clause should read as:** Solution should support to block external devices like USB, Infrared, and Bluetooth.	No Change
14	Softcell	Annexure A-Tech Spec, 6.6 Antivirus, 6.6.1 Antivirus Specification Pg no-38	Solution should be able to provide permission to access authorized external devices based on privileges.	This is OEM specfic point and restrictive in nature. Kindly delete this point.	Specification is favoring particular OEM and restritive in nature. Please dilute mention specification as per suggestion to allow our participation. **The clause should read as:** Solution should be able to provide permission to access authorized external devices based on privileges/serial id of external device	**Revised Clause:** Solution should be able to provide permission to access authorized external devices based on privileges/serial id of external device

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Page No., Clause No.	Description	Vendor		MSETCL
				Querry/Clarification	Changes Required	Revision & Comments
15	Softcell	Annexure A-Tech Spec, 6.6 Antivirus, 6.6.1 Antivirus Specification Pg no-39	Solution should support following Operating Systems: Linux (list all supported variants/versions). MaC OS (list all supported versions). Windows OS (list all supported versions). Solution Should be IPV6 attacks Ready.	This is OEM specfic point and restrictive in nature. Kindly delete this point.	Specification is favoring particular OEM and restritive in nature. Please dilute mention specification as per suggestion to allow our participation. **The clause should read as:** Solution should support following Operating Systems: Linux (list all supported variants/versions). MaC OS (list all supported versions). Windows OS (list all supported versions). Solution Should be IPV6 attacks Ready.	No Change

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Page No., Clause No.	Description	Vendor		MSETCL
				Querry/Clarification	Changes Required	Revision & Comments
16	Softcell	Annexure A-Tech Spec, 6.4.2 EDR Specifications Pg no-25	Technical Specification	This is OEM specfic point and restrictive in nature. Kindly delete this point.	Functional specifications is favoring particular OEM and restritive in nature. Please find generic functional specification to allow wider participation of OEMs. Should be capable of Powerful Investigative Capabilities (EDR) including : • Investigation and IOC Sweeping (server-side metadata sweep) • Patient Zero ID / Root Cause Analysis and IOA Behavior Hunting/Detection • API's for query / automation and Unknown file guidance • Variant Protection to detects mutations of malicious samples by recognizing known fragments of malware code • Packer Detection to Identifies packed malware in memory as it unpacks, prior to execution • Runtime Machine Learning scores real-time behavior against a cloud model to detect previously unknown	No Change

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Page No., Clause No.	Description	Vendor		MSETCL
				Querry/Clarification	Changes Required	Revision & Comments
17	Softcell	Annexure A-Tech Spec,6.2.2 Anti-APT solution specifications pg no-19	The Anti-APT solution offered must be rated as ‘leaders’ or 'Challengers' in the Gartner Magic Quadrant published by Gartner from last three years.	APT is not in Gartner	Gartner do not publish report on Anti APT solution. Hence please consider latest NSS report which is being accepted globally to assess Anti APT solutions.	**Revised Clause:** The Anti-APT solution offered must be rated as Top Player or specialist in Redicati APT production quadrant published by Redicati in any of last 3 years or Anti-APT solution operating system must be NIAP (National Information Assurance Partnership) Common Criteria certified.

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Page No., Clause No.	Description	Vendor		MSETCL
				Querry/Clarification	Changes Required	Revision & Comments
18	Softcell	**Document:** Annexure A-Tech Spec 6.3 WAF Solution **Page:** 22: Point 1	The WAF solution offered must be rated as ‘leaders’ or 'Challengers' in the Gartner Magic Quadrant published by Gartner from last three years.		Gartner Magic Quadrant is majorly inclined towards Commercial/Market coverage and less on technology. Other reports like Forrester Wave is inclined towards Technical capabilities to block attacks incase of attacks and deployment/ Market Coverage **Hence request to consider below specs** The WAF solution offered must be rated as ‘leaders’ or 'Challengers' in the Gartner Magic Quadrant/ Forrester Wave published by Gartner from last three years	**Revised Clasue:** The WAF solution offered must be rated as ‘leaders’ or 'Challengers' in the Gartner Magic Quadrant published by Gartner in atleast any one of the last three years / The WAF solution offered should be STQC tested
19	Softcell	**Document:** Annexure A-Tech Spec 6.3 WAF Solution **Page:** 22: Point 6	The solution shall have controls for Anti Web Defacement and provide ability to check the authorized version of the website content		Anti Web Defacement prevention is not possible via WAF appliances since this kind of attacks can be easily done via DNS hijacking alone which WAF Solution cannot detect **Hence request to delete the specs**	No Change

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Page No., Clause No.	Description	Vendor		MSETCL
				Querry/Clarification	Changes Required	Revision & Comments
20	Softcell	**Document:** Annexure A-Tech Spec 6.3 WAF Solution **Page:** 24: Point 20	Solution must have anti-bot protection, Brute force protection with session tracking, Data Guard protection for Information leakage protection and advanced detection methods like- TPS (Transaction per Second) and JavaScript, CAPTCHA Challenge and device fingerprinting.		CAPTCHA is old technology to prevent BOTs and can be easily bypassed via automation tools https://dev.to/tngeene/how-to-bypass-captcha-with-2captcha-and-selenium-using-python-1p9c **Hence request to modify the specs to below** Solution must have anti-bot protection, Brute force protection with session tracking, Data Guard protection for Information leakage protection and advanced detection methods like- TPS (Transaction per Second) and JavaScript/ CAPTCHA Challenge and device fingerprinting.	**Revised Clause:** Solution must have anti-bot protection, Brute force protection with session tracking, Data Guard protection for Information leakage protection and advanced detection methods like- TPS (Transaction per Second) and JavaScript/ CAPTCHA Challenge and device fingerprinting.

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Page No., Clause No.	Description	Vendor		MSETCL
				Querry/Clarification	Changes Required	Revision & Comments
21	Softcell	**Document:** Annexure A-Tech Spec 6.3 WAF Solution **Page:** 24: Point 23	The proposed solution must have load balancing for Layer-4 & layer-7, TCP Optimization, H/W compression, caching, SSL offloading capability and must protect against FTP, SMTP, HTTP, HTTPS and Application layer Dos and DDOS attacks including stress-based DOS and Heavy URL attacks and should also support SSL VPN functionality.		Web Application Firewall is meant to handle Web based traffic to inspect and block malicious traffic If a Bad Actor attacks infrastructure via DDoS as attack vector - Datacenter can be easily brought down even before it reaches WAF And DDoS attack vector targets Stateful appliances where Firewall/ WAF/ IPS etc. are all Stateful in nature SSL VPN is altogether different technology and not related to WAF **Hence request to change the specs to below** The proposed solution must have load balancing for Layer-4 & layer-7, TCP Optimization, H/W compression, caching, SSL offloading capability and must protect against HTTP, HTTPS and Application layer Dos and Heavy URL attacks.	**Revised Clause:** The proposed solution must have load balancing for Layer-4 & layer-7, TCP Optimization, H/W compression, caching, SSL offloading capability and must protect against HTTP, HTTPS and Application layer Dos and Heavy URL attacks.

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Page No., Clause No.	Description	Vendor		MSETCL
				Querry/Clarification	Changes Required	Revision & Comments
22	Softcell	**Document:** Annexure A-Tech Spec 6.3 WAF Solution **Page:** 24: Point 24	The solution should be able to encrypt the user credentials in real time i.e., when the user is typing the credentials for the web application in his/her browser for any web application that is behind the application security solution. This feature should be agentless and should not require installation of any kind of software either on client end or on the application end.		Encrypting user Credential solves only one problem i.e. protecting users from Man in The Middle attack which is anyways taken care by SSL encryption Other than that it is of no use, since a bad actor can simple consider Hash as Password and initiate attack bypass **Hence request to delete the specs**	To be removed
23	Softcell	**Document:** Annexure A-Tech Spec 6.3 WAF Solution **Page:** 24: Point 25	The proposed WAF must have Application layer encryption service to protect credentials and sensitive fields and support encryption of credentials on real time at client/browser level to ensure the protection from credential-based attack.		Encrypting user Credential solves only one problem i.e. protecting users from Man in The Middle attack which is anyways taken care by SSL encryption Other than that it is of no use, since a bad actor can simple consider Hash as Password and initiate attack bypass **Hence request to delete the specs**	No Change

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

Sr. No.	Vendor	Page No., Clause No.	Description	Vendor		MSETCL
				Querry/Clarification	Changes Required	Revision & Comments
24	Softcell	**Document:** Annexure A-Tech Spec 6.3 WAF Solution **Page:** 25: Point 27	The proposed solution must provide protection against attacks designed to abuse the application functionality. the solution must offer visibility into synthetic traffic originated by bots and legit human traffic. SI must design and size the solution for both web and mobile based application using mobile SDK.		To Protect the traffic BOT attacks need additional information for sizing since it's a dedicated technology which needs to be factored How many request per month volume is expected to be protected ? How many applications is supposed to be protected ? Are we ok to connect the solution with Cloud for AI/ML technology to leverage its intelligence to protect from advance BOT	**Clarification:** **How many request per month volume is expected to be protected? -** Assume basis the Asset Inventory **How many applications is supposed to be protected ? -**
25	Softcell	**Document:** Annexure A-Tech Spec 6.3 WAF Solution **Page:** 25: Point 28	Solution must use AI/ML based algorithms to detect the anomaly in the application behavior and must not reply on old generation signature-based technologies to detect and prevent the sophisticated attacks including gift card cracking, card enumeration, skimming, password spraying, scraping, spambots & synthetic identities		To Protect the traffic BOT attacks need additional information for sizing since it's a dedicated technology which needs to be factored How many request per month volume is expected to be protected ? How many applications is supposed to be protected ? Are we ok to connect the solution with Cloud for AI/ML technology to leverage its intelligence to protect from advance BOT	**Clarification:** **Are we ok to connect the solution with Cloud for AI/ML technology to leverage its intelligence to protect from advance BOT -** Not Recommended

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

S. No	Vendor	Page No., Clause No.	Description	Clarification Sought	Revisions & Comments
1	Haltdos Inc, AKS IT Services, Resseaux Tech Pvt. Ltd	Annexure A-Technical Specification for SOC Solution, 6.3 WAF Solution, 6.3.2 WAF Solution Specifications, Page No. 22, Point No. 1	The WAF solution offered must be rated as ‘leaders’ or 'Challengers' in the Gartner Magic Quadrant published by Gartner from last three years.	This is a restrictive clause and is not letting other vendors who are not in leader or challenger quadrant or Indian local vendors to participate in the bid. Requesting to remove this point as it is restrictive in nature.	**Revised Clasue:** The WAF solution offered must be rated as ‘leaders’ or 'Challengers' in the Gartner Magic Quadrant published by Gartner in atleast any one of the last three years / The WAF solution offered should be STQC tested
2		New Addition	**Additional Specification:** The proposed solution should have built-in API gateway with support for various authentication schemes like LDAP, JWT, Key Auth, Basic Auth, HMAC, etc.	**Reason:** 'This is an additional specification for web application firewall solution. APIs have become critical for intergation and digitization. Managing and securing APIs are as important as securing web applications. WAF solutions should have various API protection and authentication capabilities built-in to secure all web based attacks on Web and APIs.	No Change

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

S. No	Vendor	Page No., Clause No.	Description	Clarification Sought	Revisions & Comments
3		New Addition	**Additional Specification:** The solution shall able to control BOT traffic and it shall able to block known bad bots and fake search engine requests. The solution should have deception capability to implant decoys (fake links and forms) in any application without any changes to application or client.	**Reason:** 'This is an additional specification for web application firewall solution. Single biggest vector of attacks today starts with simple BOT attacks. These bots test application security, perform reconnaisance and evolve into behavior bots to perpetrate APT attacks on web based applications that are very hard to detect. Therefore, it is important to have anti-bot control features such as decoys, deception and mobile SDK in WAF to defend Web and API applications from malicious bot activities.	No Change

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

S. No	Vendor	Page No., Clause No.	Description	Clarification Sought	Revisions & Comments
4		Annexure A-Technical Specification for SOC Solution, 6.3 WAF Solution, 6.3.2 WAF Solution Specifications, Page No. 23, Point No. 17	Throughput: 10Gbps of Application Layer throughput, HTTP Request Per Second: 1M; Maximum L4 concurrent connections: 14M, Compression Throughput: 5 Gbps, SSL/TLS TPS: 4.3K with RSA 2K and 3.5K with ECC, SSL/TLS Bulk Encryption: 8Gbps, Hard drive should support 1 TB Enterprise Class HDD, appliance should support 4 X 1G (SFP) SX or LX CU ports and 2x10G (SFP+) SR or LR ports and modules should be provision form day1.	**Modification:** Throughput: 10Gbps of Application Layer throughput, HTTP Request Per Second: 1M; Maximum L4 concurrent connections: 14M, Compression Throughput: 5 Gbps, **SSL/TLS TPS: 95K with RSA 2K and 48K with ECC**, SSL/TLS Bulk Encryption: 8Gbps, Hard drive should support 2 TB Enterprise Class SDD, appliance should support 4 X 1G (SFP) SX or LX CU ports and 2x10G (SFP+) SR or LR ports and modules should be provision form day1. **Reason:** As all applications will be over HTTPS, higher SSL TPS is recommended to ensure lower latency and higher throughput performance in WAF	**Revised Clause :**Throughput: 10Gbps of Application Layer throughput, HTTP Request Per Second: 1M; Maximum L4 concurrent connections: 14M, Compression Throughput: 5 Gbps, SSL/TLS TPS: 95K with RSA 2K and 48K with ECC, SSL/TLS Bulk Encryption: 8Gbps, Hard drive should support 2 TB Enterprise Class SDD, appliance should support 4 X 1G (SFP) SX or LX CU ports and 2x10G (SFP+) SR or LR ports and modules should be provision form day1. Reason: As all applications will be over HTTPS, higher SSL TPS is recommended to ensure lower latency and higher throughput performance in WAF

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

S. No	Vendor	Page No., Clause No.	Description	Clarification Sought	Revisions & Comments
5		Annexure A- Technical Specification for SOC Solution, 6.3 WAF Solution, 6.3.2 WAF Solution Specifications, Page No. 23, Point No. 18	The solution must support integration with third party DAST tool to perform virtual patching for its protected web applications. The solution must support all the common web application vulnerability assessment tolls (Web application scanners) including Acunetix, Qualys, Rapid 7, IBM AppScan etc. to virtually patch web	**Modification:** The solution must support integration with third party DAST tool to perform virtual patching for its protected web applications. The solution must support all the common web application vulnerability assessment tolls (Web application scanners) including Acunetix, Qualys, Rapid 7, IBM AppScan etc. to virtually patch web application vulnerabilities. **In addition, the solution should provide built-in DAST tool from same OEM for faster application structure profiling and security. The built-in DAST should**	Given are minimum technical qualifications. Anything above to that is acceptable. Hence, **No Change**.
6		Annexure A- Technical Specification for SOC Solution, 6.3 WAF Solution, 6.3.2 WAF Solution Specifications, Page No. 24, Point No. 21	Web Application solution should not be virtual WAF and it should not white labeled WAF running on third party hardware. OEM of WAF product should be ISO-9001, ISO-27001, ISO-14001 certified.	**Modification:** Web Application solution should not be virtual WAF and it should not white labeled WAF running on third party hardware. OEM of WAF product should be ISO-9001, ISO-27001 certified. **Reason:** As the solution is hosted in the DC/DR and ISO-14001 is an environmental standard, hence this should not be applicable on WAF vendors	**Revised Clause :**Web Application solution should not be virtual WAF and it should not white labeled WAF running on third party hardware. OEM of WAF product should be ISO-9001, ISO-27001 certified.

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

S. No	Vendor	Page No., Clause No.	Description	Clarification Sought	Revisions & Comments
7		Annexure A-Technical Specification for SOC Solution, 6.3 WAF Solution, 6.3.2 WAF Solution Specifications, Page No. 24, Point No. 23	The proposed solution must have load balancing for Layer-4 & layer-7, TCP Optimization, H/W compression, caching, SSL offloading capability and must protect against FTP, SMTP, HTTP, HTTPS and Application layer Dos and DDOS attacks including stress-based DOS and Heavy URL attacks and should also support SSL VPN functionality.	**Modification:** The proposed solution must have load balancing for Layer-4 & layer-7, TCP Optimization, H/W compression, caching, SSL offloading capability and must protect against FTP, SMTP, HTTP, HTTPS and Application layer Dos and DDOS attacks including stress-based DOS and Heavy URL attacks. **Reason:** It is not a part of web application firewall specification and is a seperate component. Hence requesting to remove the support for SSL VPN functionality	**Revised Clause:** The proposed solution must have load balancing for Layer-4 & layer-7, TCP Optimization, H/W compression, caching, SSL offloading capability and must protect against HTTP, HTTPS and Application layer Dos and Heavy URL attacks.

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

S. No	Vendor	Page No., Clause No.	Description	Clarification Sought	Revisions & Comments
8		Annexure A-Technical Specification for SOC Solution, 6.3 WAF Solution, 6.3.2 WAF Solution Specifications, Page No. 24, Point No. 24	The solution should be able to encrypt the user credentials in real time i.e., when the user is typing the credentials for the web application in his/her browser for any web application that is behind the application security solution. This feature should be agentless and should not require installation of any kind of software either on client end or on the application end.	This is a vendor specific point and requesting to please remove the same	To be removed
9		New Addition	**Additional Specification:** The proposed solution should have built-in AV scanner and sandboxing capability. In additional it should also support integration with 3rd party sandboxing solution via API or ICAP	**Reason:** This is an additional specification for web application firewall solution to detect and mitigate any malicious file upload through web applications.	No Change

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

S. No	Vendor	Page No., Clause No.	Description	Clarification Sought	Revisions & Comments
10		New Addition	**Additional Specification:** The solution should support client certificate based authentication with capability for obtaining certificate revocation status for HTTPS client authentication	**Reason:** This is an additional specification for web application firewall solution to increase an additional authentication layer by WAF solution	No Change
11		New Addition	**Additional Specification:** The solution shall support scripting language for events based rule creation to make traffic management and security decisions using scripting language	**Reason:** This is an additional specification for web application firewall solution ensure operational excellence by automating manual tasks during traffic surge into automatic switch of solution settings and policies through alarms / events and scripts. The solution should support script in any language.	No Change

Pre Bid Quries- SP/T-0703/0322 (RFX No. 7000022437) SICTI of Cyber Security Tools for MSETCL

S. No	Vendor	Page No., Clause No.	Description	Clarification Sought	Revisions & Comments
12		New Addition	**Additional Specification:** The solution should support L4 and L7 load balancing with various LB algorithms. It should also perform periodic health checks via HTTP, TCP, UDP, SNMP and custom user defined scripts	**Reason:** This is an additional specification for web application firewall solution to enable and enhance load balancing at L4 and L7 layer. This also comes with health check to raise alerts and ensure continuity of service through list of available health web servers	No Change
13	WAF Technical Specification (Additional)	New Addition			**Additional Specification:**Proposed WAF should not be from the same OEM whose firewall is proposed in this RFP