Technical Specifications of Cyber Security Device

1.	AV	The solution may support Anti-Virus
2.	Environment	The solution shall support operating Temp. ranging from -40 to 75°C
3.	Interface	• The solution may support the inspection throughput for at least 200Mbps • The solution shall support dual WAN with combo port type (Fiber optic or copper) • The solution shall support multiple LAN ports (Minimum 04Nos ports) • The solution shall support configuration backup and upload via USB and have automation tool for offline updates.
4	IPS	• The solution shall have its Intrusion Prevention System (IPS) be used in intranet without Internet access and support customer definition; included full license & real-time signatures update.
5	Management	• The solution shall support Simple Network Management Protocol (SNMP) v1/v2/v3. • The solution shall support password strength mechanism of account management.
6	Networking	• The solution shall support DMZ function to specify physical ports as DMZ interface to allow traffic going from WAN interface to LAN interface without NAT enabled. • The solution shall support NAT passthrough function to allow traffic forwarded to the translated IP address be mapped to the real IP address of a device. • The solution shall have latency less than 500 micro-second in IPS mode. • The solution shall support Link Layer Discovery Protocol (LLDP). • The solution shall be compatible and can be deployed within PRP (Parallel Redundancy Protocol) /HSR (High-availability Seamless Redundancy) network architecture. • The solution shall support multiple account type with different permissions. • The solution shall support to be used as a switch and shall support VPN/Tunnel.
7	Operation	• The solution shall be able to select which log types to be sent to syslog server. • The solution shall support the firmware downgrade capability. • The solution shall support Active Query to discover information for hidden OT assets.

		• The solution shall support up to 32 IPS profiles for customized IPS protection.
8	Policy Enforcement	• The solution shall be able to have whitelisting function to enable packet inspection to allow/block/log incoming traffic based on pre-defined condition (IP address, service type, VLAN ID, protocol type). • The solution will need to have protocol whitelisting function to inspect and allow/block/log insecure or unexpected protocol commands from going through. • The solution needs to support multiple VLAN ID setting for one policy rule. • The solution shall support interface direction selection as one of the policy inspection rules. • The solution shall be able to inspect and to allow/block incoming packets based on pre-defined IP addresses. • The solution shall support to prevent access to specified workstation or system node.
9	Power	The solution shall have dual power inputs which can work simultaneously for power redundancy. The solution shall support power input voltage of 110–240 VDC
10	Protocol	The offered solution shall provide native, protocol-aware Deep Packet Inspection (DPI) and Granular Control Support for the industrial control system, including but not limited to IEC 60870-5-104, EtherNet/IP/CIP, MODBUS, and DNP3. Bidders shall submit a protocol-by-protocol enforcement matrix identifying the exact granularity level (command / function-code / message-type / IOA, as applicable) achieved for each protocol in use, with reference to the specific section of the product's official configuration/administration guide substantiating the claim. Claims not traceable to official product documentation shall not be considered compliant. Compliance shall not be considered satisfied solely through enforcement based on TCP/UDP port, source/destination IP address, VLAN, service or generic Layer-7 application identification.
		• The solution shall support protocols that are commonly used in communication. • TCP/IP • UDP/IP • DNP3 • IEC 60870-5-104 • IEC 61850

		• IEEE C37.118 • OSPF • BGP The solution shall support to check the packet for OT protocol format compliance
11	Protocol Filter	• The solution shall support advanced configuration on CIP (Common Industrial Protocol) protocol to allow user selecting specific select Class ID / service code to allow/deny. • The solution support SMB (Server Message Block) Granular control and shall be able to analyze SMB exchange and to block or allow frame pass according to data format (SMB v1 / SMB v2/v3) and message type. SMBv1/2/3 granular control filtering options: 1. SMB versions 2. file access permission: read only, write only, read/write. • The solution shall support up to 32 profiles for OT protocol filter.
12	Rule	The solution shall support rule editing function to have IPS profile to list out IPS rules and allow user to enable/disable individual rule with desired actions (allow & log, block & log)
13	Threat	The solution has capacity to detect Windows remote task execution/schedule and do further control. The console part includes: 1. Powershell execution. 2. schtasks/atsvc
14	USB	• The solution shall support signature update and zero configuration by USB • The solution shall allow user to manually disable the USB port via Web console
15	License Validity	• One Year License Subscription shall be provided.
16	Extension of License Subscription	• Further Two-year license subscription will be extended with same rate, terms and conditions (if required).