

(Technical Specification Compliance Sheet e-PG2-4)			
Item No.	Name of Goods	Detailed Technical Specification and Standards required	Bidder Response/Compliance Statement
1	Next Generation Firewall (High Performance on basis of Internet Traffic)		
i		Country of Origin	USA
ii		Make, and Model or Brand (when applicable)	Taiwan, FG-200G and Fortinet
iii	Next Generation Firewall (High Performance on basis of Internet Traffic)	1.Platform Requirement: The appliance-based security platform should be capable of providing firewall, application visibility, IPS, Anti-malware & Web/URL filtering functionality in a single appliance; 2.Hardware Requirements: Firewall appliance should be supplied with at least 8 x 1GE Cu Ports, 8 x 10GE SFP+ Ports, dedicated 1 x 1GE management Ports and dedicated 1 x 1GE HA Ports, The appliance hardware should be a multicore CPU architecture with a hardened 64-bit operating system,The firewall should support Active:Active & Active:Passive modes; 3.Performance & Scalability: Throughput with Firewall, IPS and Application Control enabled, Enterprise Mix traffic must be 8.5 Gbps or higher on dedicated Single appliance and not by adding Cluster of devices utilizing appmix or enterprise traffic mix transaction from day one,The NGFW Threat Protection performance by enabling functionalities of Firewall, IPS, Application Control must be 5.8 Gbps or higher on dedicated Single appliance and not by adding Cluster of devices utilizing appmix or enterprise traffic mix transaction from day one,The NGFW deep packet/SSL	Comply all mentioned Specifications

(Technical Specification Compliance Sheet e-PG2-4)			
Item No.	Name of Goods	Detailed Technical Specification and Standards required	Bidder Response/Compliance Statement
		inspection throughput must be 6 Gbps or higher on dedicated Single appliance and not by adding Cluster of devices from day one, Firewall should support at least 4000 VLANs, The NGFW should be capable to establish and maintain the privacy of communication between devices, apps or networks over the public internet using IPSEC with through of atleast 8 Gbps or Higher from day one; 4.Firewall Features: Firewall should provide application detection for DNS, FTP, HTTP, SMTP, ESMTP, LDAP, RTSP, SIP, SQLNET, H.323, SNMP, Firewall should support creating access rules with IPv4 & IPv6 objects simultaneously, Firewall should support operating in routed & transparent mode. Should support Static, RIP, OSPF, OSPFv3 and BGP Firewall should support manual NAT and Auto-NAT, static nat, dynamic NAT, dynamic pa; 5.NGFW Features:The device should allow individual users to access department's network, client-server applications, and internal network utilities and directories without the need for specialized software.Should be capable of tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.Should cater to reputation and category based URL filtering offering comprehensive alerting	



(Technical Specification Compliance Sheet e-PG2-4)			
Item No.	Name of Goods	Detailed Technical Specification and Standards required	Bidder Response/Compliance Statement
		and control over suspect web traffic and enforces policies in more than 75 categories from day one. The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.). 6. Management & Logging/Reporting: The management must be accessible via a web-based interface and ideally with no need for additional client software. The firewall should have in-built CLI option in Graphical Interface for easy access in troubleshooting & configuration. The firewall should have diagnostic CLI commands, session tracer, and packet capture for troubleshooting hardware, system, and network issues. 7. Certification & 3rd party validation: Operating system of NGFW solution must support: USGv6 / IPv6, FIPS-140-2 / Common criteria EAL4/ICSA. The OEM must be recognized as a Leader in 2022 Gartner Magic Quadrant for Enterprise Firewalls. The OEM must have 99% Security Effectiveness Score and AAA rating in threat prevention, secure sockets layer (SSL)/ transport sockets layer (TLS) functionality, stability, and reliability from CyberRatings.org independently testing for enterprise firewalls in 2023 8. Manufacturer's part number, Warranty/RMA and TAC support: Bidder must be submitted Manufacturer	



(Technical Specification Compliance Sheet e-PG2-4)			
Item No.	Name of Goods	Detailed Technical Specification and Standards required	Bidder Response/Compliance Statement
		Authorization form (MAF), Bidder should submit BOQ of device including the details part numbers, necessary TAC support 24x7 and manufacturer warranty for 1 year , Bidder should quote necessary security subscription & license for 1 year, Bidder should submit BOQ of proposed device including the details part numbers and Manufacturer's Warranty part number also have to add services " 24x7 Comprehensive Support, Firmware and General Upgrades, (Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service & Support) for One Year.	
2	Next Generation Firewall (Medium Performance)		
2(i)		Country of Origin	USA
2(ii)		Make, and Model or Brand (when applicable)	Taiwan, FG-70G and Fortinet
2(iii)	Next Generation Firewall (Medium Performance)	1. Platform Requirement: The appliance-based security platform should be capable of providing firewall, application visibility, IPS, Anti-malware & Web/URL filtering functionality in a single appliance; 2. Hardware Requirements: Firewall appliance should be supplied with at least 6 x 1GE Cu LAN Ports & 2 x 1G WAN port from day one, The appliance hardware should be a multicore CPU architecture with a hardened 64-bit operating system, The firewall should support minimum 6 Virtual firewall or	Comply all mentioned Specifications

(Technical Specification Compliance Sheet e-PG2-4)			
Item No.	Name of Goods	Detailed Technical Specification and Standards required	Bidder Response/Compliance Statement
		equivalent system from day one, The firewall should support Active:Active & Active:Passive modes; 3.Performance & Scalability: Throughput with Firewall, IPS and Application Control enabled, Enterprise Mix traffic must be 2 Gbps or higher on dedicated Single appliance and not by adding Cluster of devices utilizing appmix or enterprise traffic mix transaction from day one, The NGFW Threat Protection performance by enabling functionalities of Firewall, IPS, Application Control must be 1 Gbps or higher on dedicated Single appliance and not by adding Cluster of devices utilizing appmix or enterprise traffic mix transaction from day one, The NGFW deep packet/SSL inspection throughput must be 1 Gbps or higher on dedicated Single appliance and not by adding Cluster of devices from day one, The Single device should support at least 1 million or higher concurrent sessions, The standalone device should support 90K sessions per second from day one, Firewall should support at least 4000 VLANs, The NGFW should be capable to establish and maintain the privacy of communication between devices, apps or networks over the public internet using IPSEC with through of atleast 1.8 Gbps or Higher from day one. 4.Firewall Features: Firewall should provide application detection for DNS, FTP, HTTP, SMTP, ESMTP, LDAP, RTSP,	

(Technical Specification Compliance Sheet e-PG2-4)			
Item No.	Name of Goods	Detailed Technical Specification and Standards required	Bidder Response/Compliance Statement
		SIP, SQLNET, H.323, SNMP, Firewall should support creating access rules with IPv4 & IPv6 objects simultaneously, Firewall should support operating in routed & transparent mode. Should support Static, RIP, OSPF, OSPFv3 and BGP Firewall should support manual NAT and Auto-NAT, static nat, dynamic NAT, dynamic pa; 5.NGFW Features:The device should allow individual users to access department's network, client-server applications, and internal network utilities and directories without the need for specialized software.Should be capable of tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.Should cater to reputation and category based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies in more than 75 categories from day one.The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.). 6.Management & Logging/Reporting:The management must be accessible via a web-based interface and ideally with no need for additional client software,The firewall should have in-built CLI option in Graphical Interface for easy access in	

(Technical Specification Compliance Sheet e-PG2-4)			
Item No.	Name of Goods	Detailed Technical Specification and Standards required	Bidder Response/Compliance Statement
		troubleshooting & configuration, The firewall should have diagnostic CLI commands, session tracer, and packet capture for troubleshooting hardware, system, and network issues. 7. Certification & 3rd party validation: Operating system of NGFW solution must support: USGv6 / IPv6, FIPS-140-2 / Common criteria EAL4/ICSA. The OEM must be recognized as a Leader in 2022 Gartner Magic Quadrant for Enterprise Firewalls. The OEM must have 99% Security Effectiveness Score and AAA rating in threat prevention, secure sockets layer (SSL)/ transport sockets layer (TLS) functionality, stability, and reliability from CyberRatings.org independently testing for enterprise firewalls in 2023 8. Manufacturer's part number, Warranty/RMA and TAC support: Bidder must be submitted Manufacturer Authorization form (MAF), Bidder should submit BOQ of device including the details part numbers, necessary TAC support 24x7 and manufacturer warranty for 1 year. Bidder should quote necessary security subscription & license for 1 year. Bidder should submit BOQ of proposed device including the details part numbers and Manufacturer's Warranty part number also have to add services " 24x7 Comprehensive Support, Firmware and General Upgrades, (Unified Threat Protection (UTP) (IPS, Advanced Malware Protection,	



(Technical Specification Compliance Sheet e-PG2-4)			
Item No.	Name of Goods	Detailed Technical Specification and Standards required	Bidder Response/Compliance Statement
		Application Control, URL, DNS & Video Filtering, Antispam Service &Support) for One Year.	

