Office of the President of the Philippines
GOVERNANCE COMMISSION
FOR GOVERNMENT OWNED OR CONTROLLED CORPORATIONS
3/F, BDO Towers Paseo, 8741 Paseo De Roxas, Makati City, Philippines 1226

BAGONG PILIPINAS

BIDS AND AWARDS COMMITTEE
RESOLUTION NO. 23-0059-SBB-01
04 MARCH 2024
SUPPLEMENTAL BID BULLETIN

REVISION ON THE TERMS OF REFERENCE FOR THE PROCUREMENT OF ONE (1) LOT SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION, IMPLEMENTATION, COMMISSIONING, AND SUPPORT SERVICES FOR THE ENHANCEMENT OF GCG MAIN AND EXTENSION OFFICE NETWORK INFRASTRUCTURE

TERMS OF REFERENCE (TOR)	
ORIGINAL PROVISION	**REVISED PROVISION**
3.2.1 The bidder must provide a list of locally based manpower for the supply, delivery, installation, configuration, and commissioning of the proposed enhancement of the network infrastructure for the Main Office and Extension Office of the GCG, with each personnel being a regular employee of the bidder for at least three (3) years:	3.2.1 The bidder must provide a list of locally based manpower for the supply, delivery, installation, configuration, and commissioning of the proposed enhancement of the network infrastructure for the Main Office and Extension Office of the GCG, with each personnel being a regular employee **either** of the bidder, **bidder's product distributor, or bidder's product principal** ~~for at least three (3) years~~:
None	**3.2.3 Prior to submission of bid, the prospective bidder is required to conduct an ocular inspection of the GCG extension office located at 17th Floor BDO Towers Valero, Valero Street, Makati City. The purpose of this inspection is to allow the bidder to be familiarized with the conditions and requirements for the feasibility of the project.** **3.2.3.1 The schedule date and time for the ocular inspection will be on 07 March 2024 from 10:00 AM until 12:00 PM.** **3.2.3.2 Attendance at the ocular inspection is mandatory for all prospective bidders. Failure to attend the ocular inspection will result in disqualification from the bidding process.** **3.2.3.3 The bidder must send an email request to the GCG at procurement@gcg.gov.ph on or before 06 March 2024 02:00PM to confirm their participation in the mandatory ocular inspection. The email must contain the**

	company name and the names of bidder representatives (maximum of 2). This is to secure in advance the required gate pass and permit to enter the office building prior to the scheduled date of ocular inspection. **3.2.3.4 The bidder must obtain a Certificate of Appearance as proof of their attendance at the ocular inspection. The certificate shall be issued by the designated representative of the GCG present during the inspection.** **3.2.3.5 The Certificate of Appearance must be included in the bidder's submission along with the bid documents. Bids submitted without the Certificate of Appearance will be considered as non-compliant.** **3.2.3.6 The GCG reserves the right to verify the accuracy of the information provided in the Certificate of Appearance. Any falsification of attendance will result in disqualification and other appropriate actions.**

CLARIFICATIONS	
QUERY	**REMARKS**
Is the ocular inspection still required?	Yes.
How many copies of the bid shall be included in the submission?	Each bidder must submit one (1) original copy of the bid, and another eight (8) photocopies.
Is the cabling from the access switches going to the end-user workstation required for this project?	No.
Is the cabling from the access switches going to the other network equipment required for this project?	Yes. The bidder must supply, provide, and install the necessary cables to connect all network equipment (e.g. firewalls, access switches, wireless access points, etc.) to be deployed in each dedicated GCG office.
How many participants will join in the training requirements under item 5.1 of the TOR.	At least seven (7) participants.

REMINDERS
In order to conserve paper and avoid heavy and voluminous bid submission that entails unnecessary cost to the bidder, bidders are reminded of the following: ➢ There is no need to attach a copy of the legal documents enumerated in Annex A of the PhilGEPS Certificate of Registration (Platinum Membership). Bidders are only required to submit the same during post-qualification for the Technical Working Group's verification. ➢ For the statement of all its ongoing and completed government and private contracts, there is no need to attach a copy of each of the contract enumerated in the statement.

- *Bidders are directed to use the updated Statement of Conformity with Technical Specification attached as* ***Annex A.*** *Failure to adopt the prescribed form will be considered as non-compliant.*

(NON-VOTING)
EXEC. DIR. JOHANN CARLOS S. BARCENA
BAC Chairman

DIR. MICHAEL D. PABALINAS
Vice-Chairman

MARK GREGOR M. BENCITO
Member

MARIA ARSENIA P. PEREZ-TIBLANI
Member

ROUGIN ROYCE S. GUTIB
Provisional Member

(Not Present)
TEODORO ARSENIO F. PAGGABAO
Provisional Member

ANNEX A

Item	Specification	Statement of Compliance
	NETWORK INFRASTRUCTURE REQUIREMENTS	
1.1.	EXTERNAL FIREWALL CENTRAL MANAGEMENT SOLUTION FOR THE MAIN OFFICE	
1.1.1.	The bidder must provide one (1) unit of External Firewall Central Management Solution with complete accessories and satisfy the minimum requirements and specifications below.	
1.1.2.	Must have at least two (2) x 10/100/1000 ethernet ports.	
1.1.3.	Must have at least one (1) x USB port.	
1.1.4.	Must have at least one (1) x DB-9 console port.	
1.1.5.	Must have dual power supplies and must have hot swap redundant configuration.	
1.1.6.	Must have at least 16TB storage capacity in redundant array of independent disks (RAID) 5 set-up.	
1.1.7.	Must be accessed only with the web console and command line interface. No additional client software needs to be installed.	
1.1.8.	Must provide the ability to generate and deploy numerous policies to multiple Enterprises Security Platforms through intuitive policy management user interface.	
1.1.9.	Must be able to append rules at the top and the bottom of the managed Enterprises Security Platform(s). These rules shall only be editable from the proposed central management solution.	
1.1.10.	Must support the creation of templates that will be used to manage the common configurations (i.e. DNS, NTP, etc.) of all the managed Enterprises Security Platforms.	
1.1.11.	Must support the creation of global security policies that are shared to specific or all the managed Enterprises Security Platforms.	
1.1.12.	Must support the ability to create global settings in a tree hierarchy, with lower-level groups inheriting the settings of higher-level groups.	
1.1.13.	Must provide shared or global objects that can also be referenced by the managed Enterprises Security Platforms locally.	
1.1.14.	Must allow the creation of different various device groups with the flexibility to assign various Enterprises Security Platforms to these groups.	

1.1.15.	Must support a centralized manner of updating the software, application, threat, antivirus, and URL signature updates to all the managed Enterprises Security Platforms.	
1.1.16.	Must support role-based administration by allowing granular configuration of the access rights to every Enterprises Security Platform administrator or group.	
1.1.17.	Must have a reporting management system that can be generated manually or automatically. Rich reports shall be generated based on application, users, and threats or in any combination.	
1.1.18.	Must support report generation on the user activities (i.e. application usage, traffic summary, web browsing activity, etc.) for a specific user based on the user id.	
1.1.19.	Must support report generation on a manual ad-hoc or schedule (daily, weekly, monthly, etc.) basis.	
1.1.20.	Must log all administrative activities in both the web console and the command line interface.	
1.1.21.	Must allow the archiving and backup of configurations and historical logs to tapes or similar devices.	
1.1.22.	Must function as central management, monitoring, logging, and reporting for all Enterprises Security Platform in a single platform/dashboard/appliance.	
1.1.23.	Must have the capacity to initially manage up to 25 devices but expandable by just adding a license.	
1.1.24.	Must be able to manage and seamlessly integrate with the existing GCG's External Next Generation Firewalls in the Main Office (Palo Alto 3220) to the proposed Central Management Solution.	
1.1.25.	Must have three (3) years warranty, support, and subscriptions.	
1.2.	EXTERNAL FIREWALL APPLIANCE FOR THE EXTENSION OFFICE	
1.2.1.	The bidder must provide two (2) units of Next Generation Firewall (NGFW) appliances with complete accessories and satisfy the minimum requirements and specifications below.	
1.2.2.	Must have at least 2.9 Gigabit per second (Gbps) of real-world production throughput that includes application identification and layer-7 firewall.	
1.2.3.	Must have at least 1.6 Gbps real-world production threat prevention throughput with the following services enabled simultaneously: intrusion prevention, anti-malware, anti-spyware, command-and-control (C2) prevention, and application control.	
1.2.4.	Must support 300,000 maximum sessions and has the capability to support at least 51,000 new sessions per second.	

1.2.5.	Must support at least 2.2 Gbps of Internet Protocol Security (IPsec) Virtual Private Network (VPN) throughput.	
1.2.6.	Must support at least eight (8) x 10/100/1000 copper ports.	
1.2.7.	Must have at least one (1) x 10/100/1000Mbps ethernet out-of-band management ports to access the management web interface and perform administrative tasks.	
1.2.8.	Must have at least 128 GB Embedded Multi-Media Card (eMMC) disk drives.	
1.2.9.	Must include one (1) rack mountable tray for up to four appliance units.	
1.2.10.	Must be configured and deployed as high availability.	
1.2.11.	Must have three (3) years warranty, support, and subscriptions.	
1.2.12.	Must have a similar operating system (OS) with the existing external firewalls of GCG to enable seamless integration and single-pane management to the proposed Central Management Solution.	
1.2.13.	Must have the following general and functional requirements:	
1.2.13.1.	The proposed NGFW must have a security-specific OS and be built as an appliance (not on generic hardware) and shall handle traffic in a single-pass manner.	
1.2.13.2.	The proposed NGFW must have a separate and dedicated Central Processing Unit (CPU), memory, and hard drive for the control plane and the data plane. This is to avoid service interruption on the data plane when the control plane has been restarted or rebooted.	
1.2.13.3.	The proposed NGFW must use dedicated processing units and memory for the key functional areas of networking, security, threat prevention, and management.	
1.2.13.4.	The proposed NGFW must have built-in Secure Sockets Layer (SSL) decryption capability to prevent threats in SSL encrypted traffic and serve as the decryption broker to other security devices.	
1.2.13.5.	The proposed NGFW must support Layer 2, Layer 3, Tap mode, and Transparent mode simultaneously in the default systems without requiring adding virtual systems.	
1.2.13.6.	The proposed NGFW must be manageable from web-based Graphical User Interface (GUI) and Command Line Interface (CLI) without the need for external servers or appliances, at the same time with a capability to be managed centrally.	
1.2.13.7.	The proposed NGFW must have a basic malware analysis service, without any additional subscription. The firewall must forward portable executable files to malware analysis service for analysis.	

1.2.13.8.	The proposed NGFW must support application detection which determines what an application is irrespective of port, protocol, encryption (SSH or SSL) or any other evasive tactic used by the application. Also, must support multiple classification mechanisms such as application signatures, application protocol decoding, and heuristics to your network traffic stream to accurately identify applications.	
1.2.14.	Must have the following machine learning capabilities:	
1.2.14.1.	The proposed NGFW must support inline machine learning (ML)-based web security engines to prevent evasive and unknown web threats.	
1.2.14.2.	The proposed NGFW ML model must be able to detect malicious content by evaluating file details, including decoder fields and patterns, formulating a high probability classification and verdict.	
1.2.14.3.	The proposed NGFW must support inline ML-based protection to detect malicious Portable Executable (PE), Executable and Linkable Format (ELF), Microsoft (MS) Office files, MS PowerShell scripts, and other shell scripts in real-time.	
1.2.14.4.	The proposed NGFW ML model must dynamically detect malicious files of a specific type by evaluating file details, including decoder fields and patterns, to formulate a high probability classification of a file. This protection extends to currently unknown as well as future variants of threats.	
1.2.14.5.	The proposed NGFW must support a cloud-delivered security service that works in conjunction with the existing threat prevention capabilities to deliver protections for evasive C2 threats using real-time traffic inspection via inline deep learning detection models.	
1.2.14.6.	The proposed NGFW cloud-delivered deep learning models must support analysis of C2 threats over Hypertext Transfer Protocol (HTTP), HTTP2, SSL, unknown User Datagram Protocol (UDP) and unknown Transmission Control Protocol (TCP) applications.	
1.2.14.7.	The proposed NGFW must support inline deep learning detection engines via threat prevention cloud to analyze traffic for command injection and structured query language (SQL) injection vulnerabilities in real-time to protect users against zero-day threats.	
1.2.14.8.	The proposed NGFW must support inline deep learning detection engines profile for SQL injection and command injection.	
1.2.15.	Must have the following advanced threat prevention:	
1.2.15.1.	The proposed NGFW must support extensive (i.e. all threat signatures and heuristics rated as Low, Medium, High and Critical Severity enabled) threat prevention capabilities. Threat prevention throughput is calculated with firewall, application ID,	

	vulnerability protection, anti-virus, anti-spyware enabled concurrently on the same physical appliance.	
1.2.15.2.	The proposed NGFW must be capable of supporting and analyzing network traffic regardless of ports or encryption with full visibility, including web traffic (both HTTP, HTTP/2 and SSL), all email protocols (Simple Mail Transfer Protocol [SMTP], Simple Mail Transfer Protocol Secure [SMTPS], Internet Messaging Access Protocol [IMAP], Post Office Protocol [POP]), File Transfer Protocol (FTP), and Server Message Block (SMB) traffic to detect or prevent malicious malware and activity.	
1.2.15.3.	The proposed NGFW must have the capability to sinkhole Domain Name System (DNS) request for blacklisted or malicious domains to a configured destination Internet Protocol (IP) address.	
1.2.15.4.	The proposed NGFW must perform stream-based anti-virus and anti-spyware, and not store and forward traffic inspection.	
1.2.15.5.	The proposed NGFW must have a correlation engine that looks for predefined indicators of compromise network-wide, correlates matched indicators, and automatically highlights compromised hosts, reducing the need for manual data mining.	
1.2.15.6.	The proposed NGFW must have credential theft and abuse prevention capability.	
1.2.15.7.	The proposed NGFW must support an out of the box intrusion prevention system (IPS) signature converter plugin to automatically convert rules for Snort and Suricata IPS software into custom threat signatures.	
1.2.15.8.	The proposed NGFW must have the capability to determine the endpoint IP address that requested the blacklisted or malicious domains even when the request is proxied through an internal DNS server.	
1.2.16.	Must have the following advanced threat analysis:	
1.2.16.1.	The proposed NGFW must have inline machine learning to secure against unknown threats in real-time.	
1.2.16.2.	The proposed NGFW must be able to attain sandbox verdicts in real-time.	
1.2.16.3.	The proposed NGFW must be able to identify unknown malware by using multi-method detection technology, such as static, dynamic, and bare metal analysis.	
1.2.16.4.	The proposed NGFW must support dynamic analysis of the following file types: email links, Android Package Kit (APK), Adobe Flash, Java archive (JAR), MS Office files, PE, Portable Document Format (PDF), Mac OS files, Linux ELF files, RAR, and Zip.	
1.2.16.5.	The proposed NGFW must be able to support automatic creation and delivery of protection signatures from the threats seen in other customers as frequently as every five (5) minutes.	

1.2.16.6.	The proposed NGFW must have the capability of detecting zero-day threats in various sandboxing virtual machines with operating systems such as Windows, Mac OS, and Android.	
1.2.16.7.	The proposed NGFW must be able to provide an on-box reporting of unknown malware (i.e. replication behavior, C2 server information, file downloading, etc.).	
1.2.16.8.	The proposed NGFW must be able to provide context around attacks, such as who is the attacker, the campaigns it is involved in, and including which industries are being targeted.	
1.2.16.9.	The proposed NGFW must have indicators of compromise (IOC) tagging for alerting organizations when a specific threat has been observed in the organization or similar industry. The tags must be searchable, allowing the user to instantly pivot to associated malicious samples.	
1.2.17.	Must have the following advanced URL filtering:	
1.2.17.1.	The proposed NGFW must have natively integrated Uniform Resource Locator (URL) filtering capabilities.	
1.2.17.2.	The proposed NGFW must support locally defined URL entries / categories.	
1.2.17.3.	The proposed NGFW must have an automated cloud-based dynamic URL categorization for classifying unknown web sites.	
1.2.17.4.	The proposed NGFW must have a specific category for Malware, Phishing, Command-and-Control, Proxy Avoidance and Anonymizers, among other usual web categories.	
1.2.17.5.	The proposed NGFW must support multi-category URL filtering capabilities that includes risk category for a more granular URL categorization.	
1.2.17.6.	The proposed NGFW must have inline ML-based web content analysis for real-time detection of never-before-seen malicious and highly evasive URLs. The ML models must be retrained frequently, ensuring protection against new and evolving never before-seen threats (e.g., phishing, exploits, fraud, C2).	
1.2.17.7.	The proposed NGFW must have anti-evasion measures that protect against evasive techniques such as cloaking, fake Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA)s, and Hypertext Markup Language (HTML) character encoding.	
1.2.17.8.	The proposed NGFW must have real-time detection and prevention of credential theft by controlling sites to which users can submit corporate credentials based on the site's URL category.	
1.2.17.9.	The proposed NGFW must have phishing image detection that uses ML models to analyze images in webpages to determine whether they are imitating brands commonly used in phishing attempts.	

1.2.17.10.	The proposed NGFW must have the capability to support selective SSL decryption based on specific URL categories to reduce risk and at the same time maintain end user data privacy. For example: Decrypt specific URL categories (e.g., social networking, web-based email, content delivery networks) and exempt government, banking institution, healthcare provider URL categories from decryption.	
1.2.18.	Must have the following DNS security:	
1.2.18.1.	The proposed NGFW must stop known and unknown DNS traffic with machine learning and predictive analytics.	
1.2.18.2.	The proposed NGFW must help identify systems that are infected/ compromised by sinkholing DNS request to a C2 server.	
1.2.18.3.	The proposed NGFW must protect against Domain Generation Algorithms (DGA) based attacks which generate random domains on the fly for malware to use as a way to call back to a C2 server. Also, it must identify DGA domains based on dictionary words.	
1.2.18.4.	The proposed NGFW must protect against DNS tunneling based attacks that utilizes crafted DNS queries and response to hide malware delivery, command-and control traffic or data exfiltration/extraction.	
1.2.18.5.	The proposed NGFW must protect against ultra-low/slow DNS tunnels that spread tunneled data and exploits across multiple domains and use very slow rates to evade detection, stealing data or sending additional malicious payloads into your network.	
1.2.18.6.	The proposed NGFW must protect against strategically aged domains using predictive analytics. It must protect users from connecting to domains that were reserved and left dormant for months before use by malicious actors.	
1.2.18.7.	The proposed NGFW must prevent fast flux, technique cybercriminals use to cycle through bots and DNS records. Fast flux networks are used for phishing, malware distribution, scams, and botnet operations.	
1.2.18.8.	The proposed NGFW must protect against domains surreptitiously added to hacked DNS zones of reputable domains.	
1.2.18.9.	The proposed NGFW must prevent DNS rebinding attacks, which can be used to move laterally and attack services inside the corporate network from the internet.	
1.2.18.10.	The proposed NGFW must prevent dangling DNS attacks, which take advantage of stale DNS zone data to take over domains and cause reputational harm or launch phishing attacks.	
1.2.18.11.	The proposed NGFW must support the following DNS security categories: C2, Dynamic DNS (DDNS), malware, newly	

	registered domains, phishing, grayware, parked, and proxy avoidance & anonymizers.	
1.2.19.	Must have the following software-defined wide area network (SDWAN) capabilities:	
1.2.19.1.	The proposed NGFW must be capable as the next generation secure-SDWAN.	
1.2.19.2.	The proposed NGFW must support dynamic, intelligent path selection based on applications and services and the conditions of links that each application or service is allowed to use. The path health monitoring for each link includes latency, jitter, and packet loss.	
1.2.19.3.	The proposed NGFW must support security features, such as user and application identification/control, to provide complete traffic and security control.	
1.2.19.4.	The proposed NGFW must support link bundling of different Internet Service Provider (ISP).	
1.2.19.5.	The proposed NGFW must support the following types of WAN connections that terminates as ethernet to the device's interface: ADSL/DSL, cable modem, ethernet, fiber, LTE/3G/4G/5G, MPLS, microwave/radio, satellite, Wi-Fi, and anything that terminates as ethernet to the device's interface.	
1.2.19.6.	The proposed NGFW must support path quality profile for each set of business-critical and latency-sensitive applications, application filters, application groups, services, service objects and service group objects that has unique network quality (health) requirements based on latency, jitter, and packet loss percentage.	
1.2.19.7.	The proposed NGFW must have predefined path quality profiles, such as general-business, VOIP-video, file-sharing, audio-streaming, photo-video, and remote-access, and more.	
1.2.19.8.	The proposed NGFW must be able to monitor business-critical Software as a Service (SaaS) application to monitor the latency, jitter, and packet loss and able to swap from available WAN links to ensure application usability.	
1.2.19.9.	The proposed NGFW must support forward error correction.	
1.2.19.10.	The proposed NGFW must support packet duplication.	
1.2.19.11.	The proposed NGFW must have SD-WAN traffic distribution profiles, such as: Best Available Path, Top-Down Priority, and Weighted Session Distribution.	
1.2.19.12.	The proposed NGFW must have direct internet access (DIA) SD-WAN.	
1.2.19.13.	The proposed NGFW must support Hub-and-Spoke topology.	
1.2.19.14.	The proposed NGFW must support Full Mesh topology.	

1.2.19.15.	The proposed NGFW must be managed in the central management console.	
1.2.19.16.	The proposed NGFW must have a dashboard for visibility into your SD-WAN links and performance so that the administrator can adjust the path quality thresholds and other aspects of SD-WAN to improve its performance.	
1.2.19.17.	The proposed NGFW must have centralized statistics and reporting including application and link performance statistics, path health measurements and trend analysis, and focused views of application and link issues.	
1.2.20.	Must have the following secure remote access:	
1.2.20.1.	The proposed NGFW must have enterprise-grade protection for the mobile workforce.	
1.2.20.2.	The proposed NGFW must be able protect the remote user against unknown threats using inline machine-learning.	
1.2.20.3.	The proposed NGFW must have reliable user identification by supporting integration with Lightweight Directory Access Protocol (LDAP) and Remote Authentication Dial-In User Service (RADIUS).	
1.2.20.4.	The proposed NGFW must be able to provide accurate host information for visibility and policy enforcement.	
1.2.20.5.	The proposed NGFW must be able to check if the endpoint has customized host conditions specifically the registry entries and certain running software.	
1.2.20.6.	The proposed NGFW must be capable of enforcing pre-logon and on-demand VPN connection.	
1.2.20.7.	The proposed NGFW must be able to check if the endpoint has disk encryption configuration.	
1.2.20.8.	The proposed NGFW must be capable of clientless VPN.	
1.2.20.9.	The proposed NGFW must be able to identify if the endpoint is managed or unmanaged.	
1.2.20.10.	The proposed NGFW must be able to detect and prevent devices from connecting if certain anti-malware software is not installed.	
1.2.20.11.	The proposed NGFW must support at least the following operating systems: Windows, macOS, iOS, Android, and Chrome OS.	
1.3.	CORE SWITCH FOR THE EXTENSION OFFICE	
1.3.1.	The bidder must provide two (2) units of Core Switch (CS) with complete accessories and satisfy the minimum requirements and specifications below.	
1.3.2.	Must be a Layer 3 stackable switch with Border Gateway Protocol (BGP), Ethernet VPN (EVPN), Virtual eXtensible Local-Area Network (VXLAN), Virtual Routing and Forwarding (VRF),	

	and Open Shortest Path First (OSPF) with robust security and Quality of service (QoS).	
1.3.3.	Must have at least 880 Gbps system switching capacity, 660 Mega Packet Per Second (Mpps) system throughput, and up to 200 Gbps stacking bandwidth.	
1.3.4.	Must be a 1U rack mountable switch with full density 1GB and enhanced small form-factor pluggable (SFP+) models.	
1.3.5.	Must have built-in high speed 1/10/25/50G SFP+ uplinks.	
1.3.6.	Must have three (3) years warranty, support, and subscriptions.	
1.3.7.	Must have intelligent monitoring, visibility, and remediation with analytics engine.	
1.3.8.	Must be manageable via single pane of glass across wired, wireless, and WAN.	
1.3.9.	Must support automated configuration and verification.	
1.3.10.	Must enable secure and simple access for users and Internet of Things (IoT).	
1.3.11.	Must have the following QoS requirements:	
1.3.11.1.	The proposed CS must support Strict Priority (SP) queuing and Deficit Weighted Round Robin (DWRR).	
1.3.11.2.	The proposed CS must have traffic prioritization (IEEE 802.1p) for real-time classification into 8 priority levels that are mapped to 8 queues.	
1.3.11.3.	The proposed CS transmission rates of egressing frames can be limited on a per-queue basis using Egress Queue Shaping (EQS).	
1.3.12.	Must have the following Resiliency and High Availability requirements:	
1.3.12.1.	The proposed CS must have high performance front plane stacking for up to 10 switches.	
1.3.12.2.	The proposed CS must have the flexibility to mix both modular and fixed models within a single stack.	
1.3.12.3.	The proposed CS must have hot swappable power supplies.	
1.3.12.4.	The proposed CS must provide N+1 and N+N redundancy for high reliability in the event of power line or supply failures.	
1.3.12.5.	The proposed CS must support Virtual Router Redundancy Protocol (VRRP) that allows groups of two routers to dynamically back each other up to create highly available routed environments.	
1.3.12.6.	The proposed CS must support Unidirectional Link Detection (UDLD) that monitors link connectivity and shuts down ports at both ends if unidirectional traffic is detected, preventing loops in STP-based networks.	

1.3.12.7.	The proposed CS must support IEEE 802.3ad Link Aggregation Control Protocol (LACP) that supports up to 54 link aggregation groups (LAGs), each with eight links per group with a user-selectable hashing algorithm.	
1.3.12.8.	The proposed CS must support Microsoft Network Load Balancer (NLB) for server applications.	
1.3.12.9.	The proposed CS must support Ethernet Ring Protection Switching (ERPS) that provides rapid protection and recovery in a ring topology.	
1.3.12.10.	The proposed CS must support IEEE 802.1s Multiple Spanning Tree that provides high link availability in VLAN environments where multiple spanning trees are required; and legacy support for IEEE 802.1d and IEEE 802.1w.	
1.3.13.	Must have the following Performance and Connectivity requirements:	
1.3.13.1.	The proposed CS must have up to 880 Gbps in non-blocking bandwidth and up to 660 Mpps for forwarding.	
1.3.13.2.	The proposed CS must support 1/10/25/50G uplinks and large ternary content-addressable memory (TCAM) sizes ideal for mobility and IoT deployments in large campuses with several thousand clients.	
1.3.13.3.	The proposed CS must have 24 x 10/100/1000 BASE-T ports and 4 x 1/10/25/50G SFP+ ports.	
1.3.13.4.	The proposed CS must have at least one (1) x USB-C console port.	
1.3.13.5.	The proposed CS must have at least one (1) x OOBM port.	
1.3.13.6.	The proposed CS must have at least one (1) x USB Type A host port.	
1.3.13.7.	The proposed CS must have at least one (1) x Bluetooth dongle to be used with mobile applications.	
1.3.13.8.	The proposed CS must have jumbo frames that allow for high-performance backups and disaster-recovery systems; provides a maximum frame size of 9,198 bytes.	
1.3.13.9.	The proposed CS must have packet storm protection against broadcast and multicast storms with user-defined thresholds.	
1.3.13.10.	The proposed CS must have smart link that enables simple, fast converging link redundancy, and load balancing with dual uplinks avoiding Spanning Tree complexities.	
1.3.14.	Must have the following Management requirements:	
1.3.14.1.	The proposed CS must have scalable application specific integrated circuit (ASIC)-based wire speed network monitoring and accounting with no impact on network performance; The network administrators can gather a variety of network statistics and information for capacity planning and real time network monitoring purposes.	

1.3.14.2.	The proposed CS management interface must control, enable, or disable each of the following depending on security preferences, console port, or reset button.	
1.3.14.3.	The proposed CS must have industry standard CLI with a hierarchical structure for reduced training time and expense. Delivers increased productivity in multivendor environments.	
1.3.14.4.	The proposed CS management security restricts access to critical configuration commands, provides multiple privilege levels with password protection, and local and remote syslog capabilities allow logging of all access.	
1.3.14.5.	The proposed CS must support Simple Network Management Protocol (SNMP) v2c/v3 which provides SNMP read and trap support of industry standard Management Information Base (MIB), and private extensions.	
1.3.14.6.	The proposed CS must support remote monitoring (RMON) with standard SNMP to monitor essential network functions. Supports events, alarms, history, and statistics groups as well as a private alarm extension group; RMON, and sampled flow provide advanced monitoring and reporting capabilities for statistics, history, alarms, and events.	
1.3.14.7.	The proposed CS must support Trivial File Transfer Protocol (TFTP) and Secure File Transfer Protocol (SFTP) – offers different mechanisms for configuration updates; TFTP allows bidirectional transfers over a TCP/ IP network; SFTP runs over a Secure Shell (SSH) tunnel to provide additional security.	
1.3.14.8.	The proposed CS must support Network Time Protocol (NTP) – synchronizes timekeeping among distributed time servers and clients; keeps timekeeping consistent among all clock-dependent devices within the network so the devices can provide diverse applications based on the consistent time.	
1.3.14.9.	The proposed CS must support IEEE 802.1AB Link Layer Discovery Protocol (LLDP) – advertises and receives management information from adjacent devices on a network, facilitating easy mapping by network management applications.	
1.3.14.10.	The proposed CS must support dual flash images that provides independent primary and secondary operating system files for backup while upgrading.	
1.3.14.11.	The proposed CS must be able to assign descriptive names to ports for easy identification.	
1.3.14.12.	The proposed CS multiple configuration files can be stored to a flash image.	
1.3.14.13.	The proposed CS ingress and egress port monitoring must enable more efficient network problem solving.	
1.3.14.14.	The proposed CS must support unidirectional link detection (UDLD) that monitors the link between two switches and blocks the ports on both ends of the link if the link goes down at any point between the two devices.	

1.3.14.15.	The proposed CS must support IP SLA for Voice that monitors the quality of voice traffic using the UDP jitter and UDP jitter for Voice over Internet Protocol (VoIP) tests.	
1.3.15.	Must have the following Layer 2 Switching requirements:	
1.3.15.1.	The proposed CS must have VLAN support and tagging for IEEE 802.1Q (4,094 VLAN IDs).	
1.3.15.2.	The proposed CS must have jumbo packet support that improves the performance of large data transfers; supports frame size of up to 9,198 bytes.	
1.3.15.3.	The proposed CS must support IEEE 802.1v protocol VLANs isolate select non-IPv4 protocols automatically into their own VLANs.	
1.3.15.4.	The proposed CS must support Rapid Per-VLAN Spanning Tree (RPVST+) – allows each VLAN to build a separate spanning tree to improve link bandwidth usage; is compatible with PVST+	
1.3.15.5.	The proposed CS must support Multiple VLAN Registration Protocol (MVRP) – allows automatic learning and dynamic assignment of VLANs.	
1.3.15.6.	The proposed CS must support VXLAN encapsulation protocol for overlay network that enables a more scalable virtual network deployment.	
1.3.15.7.	The proposed CS must support Bridge Protocol Data Unit (BPDU) tunnelling that transmits STP BPDUs transparently, allowing correct tree calculations across service providers, WANs, or MANs.	
1.3.15.8.	The proposed CS must support port mirroring that duplicates port traffic (ingress and egress) to a monitoring port; supports four (4) mirroring groups.	
1.3.15.9.	The proposed CS must have Spanning Tree Protocol (STP) supports standard IEEE 802.1D STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for faster convergence, and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)	
1.3.15.10.	The proposed CS must support Internet Group Management Protocol (IGMP) that controls and manages the flooding of multicast packets in a Layer 2 network.	
1.3.15.11.	The proposed CS must have IPv4 Multicast in VXLAN/EVPN overlay support which allows Protocol-Independent Multicast Sparse Mode (PIMSM)/IGMP snooping in the VXLAN overlay.	
1.3.15.12.	The proposed CS must have IPv6 VXLAN/EVPN overlay support which allows IPv6 traffic over the VXLAN overlay.	
1.3.15.13.	The proposed CS must have VXLAN Address Resolution Protocol (ARP)/ Neighbor Discovery (ND) suppression which allows minimization of ARP and ND traffic flooding within individual VXLAN segments, thus optimizing the VXLAN network.	

1.3.16.	Must have the following Layer 3 Services requirements:	
1.3.16.1.	The proposed CS must have ARP – determines the MAC address of another IP host in the same subnet; supports static ARPs.	
1.3.16.2.	The proposed CS must have a DNS – provides a distributed database that translates domain names and IP addresses, which simplifies network design; supports client and server.	
1.3.16.3.	The proposed CS must support internal loopback testing for maintenance purposes and increased availability; loopback detection protects against incorrect cabling or network configurations and can be enabled on a per-port or per VLAN basis for added flexibility.	
1.3.16.4.	The proposed CS must have route maps that provide more control during route redistribution; allow filtering and altering of route metrics.	
1.3.17.	Must have the following Security requirements:	
1.3.17.1.	The proposed CS must have Access Control List (ACL) support for both IPv4 and IPv6; allows for filtering traffic to prevent unauthorized users from accessing the network, or for controlling network traffic to save resources; rules can either deny or permit traffic to be forwarded; rules can be based on a Layer 2 header or a Layer 3 protocol header.	
1.3.17.2.	The ACLs must also provide filtering based on the IP field, source/ destination IP address/subnet, and source/ destination TCP/UDP port number on a per-VLAN or per-port basis.	
1.3.17.3.	The proposed CS must have management access security for both on- and off-box authentication for administrative access. RADIUS or Terminal Access Controller Access Control System (TACACS)+ can be used to provide encrypted user authentication. Additionally, TACACS+ can also provide admin authorization services.	
1.3.17.4.	The proposed CS must support Control Plane Policing (CoPP) which sets rate limit on control protocols to protect CPU overload from Denial-of-Service (DOS) attacks.	
1.3.17.5.	The proposed CS must have support for multiple user authentication methods. Uses an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards.	
1.3.17.6.	The proposed CS must support MAC-based client authentication.	
1.3.17.7.	The proposed CS must have secure management access that delivers secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2, SSL, and/or SNMPv3.	
1.3.17.8.	The proposed CS must have switch CPU protection – provides automatic protection against malicious network traffic trying to shut down the switch.	

1.3.17.9.	The proposed CS must have Internet Control Message Protocol (ICMP) throttling – defeats ICMP denial-of-service attacks by enabling any switch port to automatically throttle ICMP traffic.	
1.3.17.10.	The proposed CS must have port security that allows access only to specified MAC addresses, which can be learned or specified by the network administrator.	
1.3.17.11.	The proposed CS must have MAC address lockout – prevents configured MAC addresses from connecting to the network.	
1.3.17.12.	The proposed CS must have MAC pinning – allows non-chatty legacy devices to stay authenticated by pinning client MAC addresses to the port until the client logs off or gets disconnected.	
1.3.17.13.	The proposed CS SSL must encrypt all HTTP traffic, allowing secure access to the browser-based management GUI in the switch.	
1.3.18.	Must have the following Multicast requirements:	
1.3.18.1.	The proposed CS must support IGMP – utilizes Any-Source Multicast (ASM) to manage IPv4 multicast networks; supports IGMPv1, v2, and v3.	
1.3.18.2.	The proposed CS must support IGMP Snooping – allows multiple VLANs to receive the same IPv4 multicast traffic, lessening network bandwidth demand by reducing multiple streams to each VLAN.	
1.3.18.3.	The proposed CS must support Multicast Listener Discovery (MLD) – enables discovery of IPv6 multicast listeners; support MLD v1 and v2.	
1.3.18.4.	The proposed CS must support Protocol Independent Multicast (PIM) – defines modes of IPv4 and IPv6 multicasting to allow one-to-many and many-to-many transmission of information; supports PIM Sparse Mode (SM) and Dense Mode (DM) for both IPv4 and IPv6.	
1.4.	MULTI-GIGABIT ACCESS SWITCH FOR THE EXTENSION OFFICE	
1.4.1.	The bidder must provide one (1) unit of Multi-Gigabit PoE Access Switch (MGPAS) with complete accessories and satisfy the minimum requirements and specifications below.	
1.4.2.	Must be a Layer 3 stackable switch with BGP, EVPN, VXLAN, VRF, and OSPF with robust security and QoS.	
1.4.3.	Must have at least 880 Gbps system switching capacity, 660 Mpps system throughput, and up to 200 Gbps stacking bandwidth.	
1.4.4.	Must be a 1U rack mountable switch with full density smart rate (1/2.5/5G) multi-gigabit ports, 60 watts PoE, and SFP+ models.	
1.4.5.	Must have built-in high speed 10/25/50G uplinks.	
1.4.6.	Must have three (3) years warranty, support, and subscriptions.	

1.4.7.	Must have intelligent monitoring, visibility, and remediation with analytics engine.	
1.4.8.	Must be manageable via single pane of glass across wired, wireless, and WAN.	
1.4.9.	Must support automated configuration and verification.	
1.4.10.	Must enable secure and simple access for users and IoT.	
1.4.11.	Must have the following QoS requirements:	
1.4.11.1.	The proposed MGPAS must support SP queuing and DWRR.	
1.4.11.2.	The proposed MGPAS must have traffic prioritization (IEEE 802.1p) for real-time classification into 8 priority levels that are mapped to 8 queues.	
1.4.11.3.	The proposed MGPAS transmission rates of egressing frames can be limited on a per-queue basis using EQS.	
1.4.12.	Must have the following Resiliency and High Availability requirements:	
1.4.12.1.	The proposed MGPAS must have high performance front plane stacking for up to 10 switches.	
1.4.12.2.	The proposed MGPAS must have the flexibility to mix both modular and fixed models within a single stack.	
1.4.12.3.	The proposed MGPAS must have hot swappable power supplies.	
1.4.12.4.	The proposed MGPAS must provide N+1 and N+N redundancy for high reliability in the event of power line or supply failures.	
1.4.12.5.	The proposed MGPAS must support VRRP that allows groups of two routers to dynamically back each other up to create highly available routed environments.	
1.4.12.6.	The proposed MGPAS must support UDLD that monitors link connectivity and shuts down ports at both ends if unidirectional traffic is detected, preventing loops in STP-based networks.	
1.4.12.7.	The proposed MGPAS must support IEEE 802.3ad LACP that supports up to 54 LAGs, each with eight links per group with a user-selectable hashing algorithm.	
1.4.12.8.	The proposed MGPAS must support Microsoft NLB for server applications.	
1.4.12.9.	The proposed MGPAS must support ERPS that provides rapid protection and recovery in a ring topology.	
1.4.12.10.	The proposed MGPAS must support IEEE 802.1s MSTP that provides high link availability in VLAN environments where multiple spanning trees are required; and legacy support for IEEE 802.1d and IEEE 802.1w.	
1.4.13.	Must have the following Performance and Connectivity requirements:	

1.4.13.1.	The proposed MGPAS must have up to 880 Gbps in non-blocking bandwidth and up to 660 Mpps for forwarding.	
1.4.13.2.	The proposed MGPAS must support 10/25G uplinks and large TCAM sizes ideal for mobility and IoT deployments in large campuses with several thousand clients.	
1.4.13.3.	The proposed MGPAS must have 24 x smart rate (1/2.5/5G) multi-gigabit class 6 PoE ports supporting up to 60 watts per port.	
1.4.13.4.	The proposed MGPAS must have 4 x 1/10/25G SFP+ ports.	
1.4.13.5.	The proposed MGPAS must have at least one (1) x USB-C console port.	
1.4.13.6.	The proposed MGPAS must have at least one (1) x OOBM port.	
1.4.13.7.	The proposed MGPAS must have at least one (1) x USB Type A host port.	
1.4.13.8.	The proposed MGPAS must have at least one (1) x Bluetooth dongle to be used with mobile applications.	
1.4.13.9.	The proposed MGPAS must have jumbo frames that allow for high-performance backups and disaster-recovery systems; provides a maximum frame size of 9,198 bytes.	
1.4.13.10.	The proposed MGPAS must have packet storm protection against broadcast and multicast storms with user-defined thresholds.	
1.4.13.11.	The proposed MGPAS must have smart link that enables simple, fast converging link redundancy, and load balancing with dual uplinks avoiding Spanning Tree complexities.	
1.4.13.12.	The proposed MGPAS must supports PoE Standards IEEE 802.3af, 802.3at and 802.3bt (up to 60 watts).	
1.4.14.	Must have the following Management requirements:	
1.4.14.1.	The proposed MGPAS must have scalable ASIC-based wire speed network monitoring and accounting with no impact on network performance; The network administrators can gather a variety of network statistics and information for capacity planning and real time network monitoring purposes.	
1.4.14.2.	The proposed MGPAS management interface must control, enable, or disable each of the following depending on security preferences, console port, or reset button.	
1.4.14.3.	The proposed MGPAS must have industry standard CLI with a hierarchical structure for reduced training time and expense. Delivers increased productivity in multivendor environments.	
1.4.14.4.	The proposed MGPAS management security restricts access to critical configuration commands, provides multiple privilege levels with password protection, and local and remote syslog capabilities allow logging of all access.	

1.4.14.5.	The proposed MGPAS must support SNMP v2c/v3 which provides SNMP read and trap support of industry standard MIB, and private extensions.	
1.4.14.6.	The proposed MGPAS must support RMON with standard SNMP to monitor essential network functions. Supports events, alarms, history, and statistics groups as well as a private alarm extension group; RMON, and sampled flow provide advanced monitoring and reporting capabilities for statistics, history, alarms, and events.	
1.4.14.7.	The proposed MGPAS must support TFTP and SFTP – offers different mechanisms for configuration updates; TFTP allows bidirectional transfers over a TCP/ IP network; SFTP runs over an SSH tunnel to provide additional security.	
1.4.14.8.	The proposed MGPAS must support NTP – synchronizes timekeeping among distributed time servers and clients; keeps timekeeping consistent among all clock-dependent devices within the network so the devices can provide diverse applications based on the consistent time.	
1.4.14.9.	The proposed MGPAS must support IEEE 802.1AB LLDP – advertises and receives management information from adjacent devices on a network, facilitating easy mapping by network management applications.	
1.4.14.10.	The proposed MGPAS must support dual flash images that provide independent primary and secondary operating system files for backup while upgrading.	
1.4.14.11.	The proposed MGPAS must be able to assign descriptive names to ports for easy identification.	
1.4.14.12.	The proposed MGPAS multiple configuration files can be stored to a flash image.	
1.4.14.13.	The proposed MGPAS ingress and egress port monitoring must enable more efficient network problem solving.	
1.4.14.14.	The proposed MGPAS must support UDLD that monitors the link between two switches and blocks the ports on both ends of the link if the link goes down at any point between the two devices.	
1.4.14.15.	The proposed MGPAS must support IP SLA for Voice that monitors the quality of voice traffic using the UDP jitter and UDP jitter for VoIP tests.	
1.4.15.	Must have the following Layer 2 Switching requirements:	
1.4.15.1.	The proposed MGPAS must have VLAN support and tagging for IEEE 802.1Q (4,094 VLAN IDs).	
1.4.15.2.	The proposed MGPAS must have jumbo packet support that improves the performance of large data transfers; supports frame size of up to 9,198 bytes.	

1.4.15.3.	The proposed MGPAS must support IEEE 802.1v protocol VLANs isolate select non-IPv4 protocols automatically into their own VLANs.	
1.4.15.4.	The proposed MGPAS must support RPVST+ – allows each VLAN to build a separate spanning tree to improve link bandwidth usage; is compatible with PVST+	
1.4.15.5.	The proposed MGPAS must support MVRP – allows automatic learning and dynamic assignment of VLANs.	
1.4.15.6.	The proposed MGPAS must support VXLAN encapsulation protocol for overlay network that enables a more scalable virtual network deployment.	
1.4.15.7.	The proposed MGPAS must support Bridge Protocol Data Unit (BPDU) tunnelling that transmits STP BPDUs transparently, allowing correct tree calculations across service providers, WANs, or MANs.	
1.4.15.8.	The proposed MGPAS must support port mirroring that duplicates port traffic (ingress and egress) to a monitoring port; supports four (4) mirroring groups.	
1.4.15.9.	The proposed MGPAS must have STP supports standard IEEE 802.1D STP, IEEE 802.1w RSTP for faster convergence, and IEEE 802.1s MSTP.	
1.4.15.10.	The proposed MGPAS must support IGMP that controls and manages the flooding of multicast packets in a Layer 2 network.	
1.4.15.11.	The proposed MGPAS must have IPv4 Multicast in VXLAN/EVPN overlay support which allows PIMSM/IGMP snooping in the VXLAN overlay.	
1.4.15.12.	The proposed MGPAS must have IPv6 VXLAN/EVPN overlay support which allows IPv6 traffic over the VXLAN overlay.	
1.4.15.13.	The proposed MGPAS must have VXLAN ARP/ND suppression which allows minimization of ARP and ND traffic flooding within individual VXLAN segments, thus optimizing the VXLAN network.	
1.4.16.	Must have the following Layer 3 Services requirements:	
1.4.16.1.	The proposed MGPAS must have ARP – determines the MAC address of another IP host in the same subnet; supports static ARPs.	
1.4.16.2.	The proposed MGPAS must have a DNS – provides a distributed database that translates domain names and IP addresses, which simplifies network design; supports client and server.	
1.4.16.3.	The proposed MGPAS must support internal loopback testing for maintenance purposes and increased availability; loopback detection protects against incorrect cabling or network configurations and can be enabled on a per-port or per VLAN basis for added flexibility.	

1.4.16.4.	The proposed MGPAS must have route maps that provide more control during route redistribution; allow filtering and altering of route metrics.	
1.4.17.	Must have the following Security requirements:	
1.4.17.1.	The proposed MGPAS must have ACL support for both IPv4 and IPv6; allows for filtering traffic to prevent unauthorized users from accessing the network, or for controlling network traffic to save resources; rules can either deny or permit traffic to be forwarded; rules can be based on a Layer 2 header or a Layer 3 protocol header.	
1.4.17.2.	The ACLs must also provide filtering based on the IP field, source/ destination IP address/subnet, and source/ destination TCP/UDP port number on a per-VLAN or per-port basis.	
1.4.17.3.	The proposed MGPAS must have management access security for both on- and off-box authentication for administrative access. RADIUS or TACACS+ can be used to provide encrypted user authentication. Additionally, TACACS+ can also provide admin authorization services.	
1.4.17.4.	The proposed MGPAS must support CoPP which sets rate limit on control protocols to protect CPU overload from DOS attacks.	
1.4.17.5.	The proposed MGPAS must have support for multiple user authentication methods. Uses an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards.	
1.4.17.6.	The proposed MGPAS must support MAC-based client authentication.	
1.4.17.7.	The proposed MGPAS must have secure management access that delivers secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2, SSL, and/or SNMPv3.	
1.4.17.8.	The proposed MGPAS must have switch CPU protection – provides automatic protection against malicious network traffic trying to shut down the switch.	
1.4.17.9.	The proposed MGPAS must have ICMP throttling – defeats ICMP denial-of-service attacks by enabling any switch port to automatically throttle ICMP traffic.	
1.4.17.10.	The proposed MGPAS must have port security that allows access only to specified MAC addresses, which can be learned or specified by the network administrator.	
1.4.17.11.	The proposed MGPAS must have MAC address lockout – prevents configured MAC addresses from connecting to the network.	
1.4.17.12.	The proposed MGPAS must have MAC pinning – allows non-chatty legacy devices to stay authenticated by pinning client MAC addresses to the port until the client logs off or gets disconnected.	

1.4.17.13.	The proposed MGPAS SSL must encrypt all HTTP traffic, allowing secure access to the browser-based management GUI in the switch.	
1.4.18.	Must have the following Multicast requirements:	
1.4.18.1.	The proposed MGPAS must support IGMP – utilizes ASM to manage IPv4 multicast networks; supports IGMPv1, v2, and v3.	
1.4.18.2.	The proposed MGPAS must support IGMP Snooping – allows multiple VLANs to receive the same IPv4 multicast traffic, lessening network bandwidth demand by reducing multiple streams to each VLAN.	
1.4.18.3.	The proposed MGPAS must support MLD – enables discovery of IPv6 multicast listeners; support MLD v1 and v2.	
1.4.18.4.	The proposed MGPAS must support PIM – defines modes of IPv4 and IPv6 multicasting to allow one-to-many and many-to-many transmission of information; supports PIMSM and DM for both IPv4 and IPv6.	
1.5.	LAN ACCESS SWITCH FOR THE EXTENSION OFFICE	
1.5.1.	The bidder must provide four (4) units of PoE Access Switch (PAS) with complete accessories and satisfy the minimum requirements and specifications below.	
1.5.2.	Must support the ACLs, robust QoS, and common protocols such as static routing.	
1.5.3.	Must support up to eight (8) switches (or members) in a stack via chain or ring topology.	
1.5.4.	Must be capable of intelligent monitoring, visibility, and troubleshooting with built-in tool.	
1.5.5.	Must be manageable via single pane of glass across wired, wireless, and WAN.	
1.5.6.	Must be capable of one touch deployment using a mobile application.	
1.5.7.	Must have support for automated configuration and verification via dedicated software.	
1.5.8.	Must have secure and simple access for users and IoT with dynamic segmentation.	
1.5.9.	Must have three (3) years warranty, support, and subscriptions.	
1.5.10.	Must have the following QoS requirements:	
1.5.10.1.	The proposed PAS must support SP queuing and DWRR.	
1.5.10.2.	The proposed PAS must have traffic prioritization (IEEE 802.1p) for real-time classification into 8 priority levels that are mapped to 8 queues.	
1.5.10.3.	The proposed PAS transmission rates of egressing frames can be limited on a per-queue basis using EQS.	

1.5.10.4.	The proposed PAS must support Class of Service (CoS) – sets the IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and Differentiated Services (DiffServ).	
1.5.10.5.	The proposed PAS must support rate limiting that sets per-port ingress enforced maximums and per-port, per-queue minimums.	
1.5.11.	Must have the following Resiliency and High Availability requirements:	
1.5.11.1.	The proposed PAS must support UDLD that monitors link connectivity and shuts down ports at both ends if unidirectional traffic is detected, preventing loops in STP-based networks.	
1.5.11.2.	The proposed PAS must support IEEE 802.3ad LACP that supports up to 54 LAGs, each with eight (8) links per group with a user-selectable hashing algorithm.	
1.5.11.3.	The proposed PAS must have IEEE 802.3ad LACP and port trunking support for static and dynamic trunks where each trunk supports up to eight links (ports) per static trunk.	
1.5.11.4.	The proposed PAS must support IEEE 802.1s MSTP that provides high link availability in VLAN environments where multiple spanning trees are required; and legacy support for IEEE 802.1d and IEEE 802.1w.	
1.5.11.5.	The proposed PAS must support VRRP that allows groups of two routers to dynamically back each other up to create highly available routed environments.	
1.5.12.	Must have the following Performance and Connectivity requirements:	
1.5.12.1.	The proposed PAS must have up to 176 Gbps in non-blocking bandwidth and up to 130.9 Mpps for forwarding.	
1.5.12.2.	The proposed PAS must have selectable queue configurations that allow for increased performance by defining a number of queues and associated memory buffering to best meet the requirements of network applications.	
1.5.12.3.	The proposed PAS must have 48 x 10/100/1000BASE-T Class 4 PoE ports, supporting up to 30 watts per port and 4 x 1/10G SFP+ ports.	
1.5.12.4.	The proposed PAS must have at least one (1) x USB-C console port.	
1.5.12.5.	The proposed PAS must have at least one (1) x OOBM port.	
1.5.12.6.	The proposed PAS must have at least one (1) x USB Type A host port.	
1.5.12.7.	The proposed PAS must have at least one (1) x Bluetooth dongle to be used with mobile applications.	

1.5.12.8.	The proposed PAS must have jumbo frames that allow for high-performance backups and disaster-recovery systems; provides a maximum frame size of 9,198 bytes.	
1.5.12.9.	The proposed PAS must have packet storm protection against broadcast and multicast storms with user-defined thresholds.	
1.5.12.10.	The proposed PAS must have smart link that enables simple, fast converging link redundancy, and load balancing with dual uplinks avoiding Spanning Tree complexities.	
1.5.12.11.	The proposed PAS must support PoE Standards IEEE 802.3af and 802.3at.	
1.5.13.	Must have the following Management requirements:	
1.5.13.1.	The proposed PAS must have a built-in programmable and easy-to-use REST API interface.	
1.5.13.2.	The proposed PAS must support simple day zero provisioning.	
1.5.13.3.	The proposed PAS must have ASIC-based wire speed network monitoring and accounting with no impact on network performance; network operators can gather a variety of network statistics and information for capacity planning and real-time network monitoring purposes.	
1.5.13.4.	The proposed PAS management interface must control, enable, or disable each of the following depending on security preferences, console port, or reset button.	
1.5.13.5.	The proposed PAS must have industry standard CLI with a hierarchical structure for reduced training time and expense. Delivers increased productivity in multivendor environments.	
1.5.13.6.	The proposed PAS management security restricts access to critical configuration commands, provides multiple privilege levels with password protection, and local and remote syslog capabilities allow logging of all access.	
1.5.13.7.	The proposed PAS must support SNMP v2c/v3 which provides SNMP read and trap support of industry standard MIB, and private extensions.	
1.5.13.8.	The proposed PAS must support RMON with standard SNMP to monitor essential network functions. Supports events, alarms, history, and statistics groups as well as a private alarm extension group; RMON, and sampled flow provide advanced monitoring and reporting capabilities for statistics, history, alarms, and events.	
1.5.13.9.	The proposed MGPAS must support TFTP and SFTP – offers different mechanisms for configuration updates; TFTP allows bidirectional transfers over a TCP/ IP network; SFTP runs over an SSH tunnel to provide additional security.	
1.5.13.10.	The proposed PAS must have debug and sampler utility supports ping and traceroute for IPv4 and IPv6.	

1.5.13.11.	The proposed PAS must support NTP – synchronizes timekeeping among distributed time servers and clients; keeps timekeeping consistent among all clock-dependent devices within the network so the devices can provide diverse applications based on the consistent time.	
1.5.13.12.	The proposed PAS must support IEEE 802.1AB LLDP – advertises and receives management information from adjacent devices on a network, facilitating easy mapping by network management applications.	
1.5.13.13.	The proposed PAS must support dual flash images that provide independent primary and secondary operating system files for backup while upgrading.	
1.5.13.14.	The proposed PAS ingress and egress port monitoring must enable more efficient network problem solving.	
1.5.13.15.	The proposed PAS must support UDLD that monitors the link between two switches and blocks the ports on both ends of the link if the link goes down at any point between the two devices.	
1.5.13.16.	The proposed PAS must support IP SLA for Voice that monitors the quality of voice traffic using the UDP jitter and UDP jitter for VoIP tests.	
1.5.14.	Must have the following Layer 2 Switching requirements:	
1.5.14.1.	The proposed PAS must have VLAN support and tagging for IEEE 802.1Q (4,094 VLAN IDs).	
1.5.14.2.	The proposed PAS must have jumbo packet support that improves the performance of large data transfers; supports frame size of up to 9,220 bytes.	
1.5.14.3.	The proposed PAS must support IEEE 802.1v protocol VLANs isolate select non-IPv4 protocols automatically into their own VLANs.	
1.5.14.4.	The proposed PAS must support RPVST+ – allows each VLAN to build a separate spanning tree to improve link bandwidth usage; is compatible with PVST+	
1.5.14.5.	The proposed PAS must support MVRP – allows automatic learning and dynamic assignment of VLANs.	
1.5.14.6.	The proposed PAS must support VXLAN encapsulation protocol for overlay network that enables a more scalable virtual network deployment.	
1.5.14.7.	The proposed PAS must support Bridge Protocol Data Unit (BPDU) tunnelling that transmits STP BPDUs transparently, allowing correct tree calculations across service providers, WANs, or MANs.	
1.5.14.8.	The proposed PAS must support port mirroring that duplicates port traffic (ingress and egress) to a monitoring port; supports four (4) mirroring groups.	

1.5.14.9.	The proposed PAS must have STP supports standard IEEE 802.1D STP, IEEE 802.1w RSTP for faster convergence, and IEEE 802.1s MSTP.	
1.5.14.10.	The proposed PAS must support IGMP that controls and manages the flooding of multicast packets in a Layer 2 network.	
1.5.15.	Must have the following Layer 3 Services requirements:	
1.5.15.1.	The proposed PAS must support loopback interface address which defines an address in OSPF, improving diagnostic capability.	
1.5.15.2.	The proposed PAS must support ARP – determines the MAC address of another IP host in the same subnet; supports static ARPs; gratuitous ARP allows detection of duplicate IP addresses; proxy ARP allows normal ARP operation between subnets or when subnets are separated by a Layer 2 network.	
1.5.15.3.	The proposed PAS must have a DNS – provides a distributed database that translates domain names and IP addresses, which simplifies network design; supports client and server.	
1.5.15.4.	The proposed PAS must support internal loopback testing for maintenance purposes and increased availability; loopback detection protects against incorrect cabling or network configurations and can be enabled on a per-port or per-VLAN basis for added flexibility.	
1.5.16.	Must have the following Security requirements:	
1.5.16.1.	The proposed PAS must be Trade Agreement Act (TAA) compliant that uses FIPS 140-2 validated cryptography for protection of sensitive information.	
1.5.16.2.	The proposed PAS must have ACL support for both IPv4 and IPv6; allows for filtering traffic to prevent unauthorized users from accessing the network, or for controlling network traffic to save resources; rules can either deny or permit traffic to be forwarded; rules can be based on a Layer 2 header or a Layer 3 protocol header.	
1.5.16.3.	The ACLs must also provide filtering based on the IP field, source/ destination IP address/subnet, and source/ destination TCP/UDP port number on a per-VLAN or per-port basis.	
1.5.16.4.	The proposed PAS must support RADIUS.	
1.5.16.5.	The proposed PAS must support TACACS+ that delivers an authentication tool using TCP with encryption of the full authentication request, providing additional security.	
1.5.16.6.	The proposed PAS must have management access security for both on- and off-box authentication for administrative access. RADIUS or TACACS+ can be used to provide encrypted user authentication. Additionally, TACACS+ can also provide admin authorization services.	

1.5.16.7.	The proposed PAS must support CoPP which sets rate limit on control protocols to protect CPU overload from DOS attacks.	
1.5.16.8.	The proposed PAS must have support for multiple user authentication methods. Uses an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards.	
1.5.16.9.	The proposed PAS must support MAC-based client authentication.	
1.5.16.10.	The proposed PAS must support concurrent IEEE 802.1X, Web, and MAC authentication schemes per switch port accepts up to 32 sessions of IEEE 802.1X, Web, and MAC authentications.	
1.5.16.11.	The proposed PAS must have secure management access that delivers secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2, SSL, and/or SNMPv3.	
1.5.16.12.	The proposed PAS SSL must encrypt all HTTP traffic, allowing secure access to the browser-based management GUI in the switch.	
1.5.16.13.	The proposed PAS must have MAC address lockout – prevents configured MAC addresses from connecting to the network.	
1.5.17.	Must have the following Multicast requirements:	
1.5.17.1.	The proposed PAS must support IGMP – utilizes ASM to manage IPv4 multicast networks; supports IGMPv1, v2, and v3.	
1.5.17.2.	The proposed PAS must support IGMP Snooping – allows multiple VLANs to receive the same IPv4 multicast traffic, lessening network bandwidth demand by reducing multiple streams to each VLAN.	
1.5.17.3.	The proposed PAS must support MLD – enables discovery of IPv6 multicast listeners; support MLD v1 and v2.	
1.5.17.4.	The proposed PAS must support PIM – defines modes of IPv4 and IPv6 multicasting to allow one-to-many and many-to-many transmission of information; supports PIM SM and DM for both IPv4 and IPv6.	
1.6.	WIRELESS ACCESS POINT FOR THE EXTENSION OFFICE	
1.6.1.	WIRELESS ACCESS POINTS FOR WORKFORCE AREA	
1.6.1.1.	The bidder must provide six (6) units of Wireless Access Point (AP) for the Workforce Area with complete accessories and satisfy the minimum requirements and specifications below.	
1.6.1.2.	Must be an indoor AP type with dual radio, 5GHz and 2.4GHz 802.11ax 4x4 Multiple Input, Multiple Output (MIMO).	
1.6.1.3.	For 5GHz radio: four (4) spatial stream (SS) HE80 (or 2SS HE160) MIMO for up to 2.4Gbps wireless data rate.	
1.6.1.4.	For 2.4GHz radio: four (4) SS HE40 (HE20) MIMO for up to 1,147Mbps wireless data rate.	

1.6.1.5.	Must have three (3) years warranty, support, and subscriptions.	
1.6.1.6.	Must support at least up to 1,024 associated client devices per radio, and up to 16 Basic Service Set Identifier (BSSID)s per radio.	
1.6.1.7.	Must support the following frequency bands:	
1.6.1.7.1.	2.400 to 2.4835GHz	
1.6.1.7.2.	5.150 to 5.250GHz	
1.6.1.7.3.	5.250 to 5.350GHz	
1.6.1.7.4.	5.470 to 5.725GHz	
1.6.1.7.5.	5.725 to 5.850GHz	
1.6.1.8.	Must support the dynamic frequency selection (DFS) which optimizes the use of available radio frequency (RF) spectrum.	
1.6.1.9.	Must support the following radio technologies:	
1.6.1.9.1.	802.11b: Direct-sequence spread-spectrum (DSSS)	
1.6.1.9.2.	802.11a/g/n/ac: Orthogonal frequency-division multiplexing (OFDM)	
1.6.1.9.3.	802.11ax: Orthogonal frequency-division multiple access (OFDMA) with up to thirty-seven (37) resource units (for an 80MHz channel)	
1.6.1.10.	Must support the following modulation types:	
1.6.1.10.1.	802.11b: BPSK, QPSK, CCK	
1.6.1.10.2.	802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM	
1.6.1.10.3.	802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM	
1.6.1.10.4.	802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM	
1.6.1.11.	Must support 802.11n high-throughput support: HT20/40.	
1.6.1.12.	Must support 802.11ac very high throughput support: VHT20/40/80/160.	
1.6.1.13.	Must support 802.11ax high efficiency support: HE20/40/80/160.	
1.6.1.14.	Must support the following data rates (Mbps):	
1.6.1.14.1.	802.11b: 1, 2, 5.5, 11	
1.6.1.14.2.	802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54	
1.6.1.14.3.	802.11n: 6.5 to 600 (MCS0 to MCS31, HT20 to HT40), 800 with 256-QAM	

1.6.1.14.4.	802.11ac: 6.5 to 1,733 (MCS0 to MCS9, NSS = 1 to 4, VHT20 to VHT160), 2,166 with 1024-QAM	
1.6.1.14.5.	802.11ax (2.4GHz): 3.6 to 1,147 (MCS0 to MCS11, NSS = 1 to 4, HE20 to HE40)	
1.6.1.14.6.	802.11ax (5GHz): 3.6 to 2,402 (MCS0 to MCS11, NSS = 1 to 4, HE20 to HE160).	
1.6.1.15.	Must support 802.11n/ac packet aggregation: A-MPDU, A-MSDU.	
1.6.1.16.	Must have transmit power that is configurable in increments of 0.5 dBm.	
1.6.1.17.	Must support the following maximum transmit power:	
1.6.1.17.1.	2.4 GHz band: +24 dBm (18dBm per chain)	
1.6.1.17.2.	5 GHz band: +24 dBm (18 dBm per chain)	
1.6.1.18.	Must support Advanced Cellular Coexistence (ACC) which minimizes the impact of interference from cellular networks.	
1.6.1.19.	Must support maximum ratio combining (MRC) for improved receiver performance.	
1.6.1.20.	Must support cyclic delay/shift diversity (CDD/CSD) for improved downlink RF performance.	
1.6.1.21.	Must support space-time block coding (STBC) for increased range and improved reception.	
1.6.1.22.	Must support low-density parity check (LDPC) for high-efficiency error correction and increased throughput.	
1.6.1.23.	Must support transmit beam-forming (TxBF) for increased signal reliability and range.	
1.6.1.24.	Must support 802.11ax Target Wait Time (TWT) to support low-power client devices.	
1.6.1.25.	Must have four integrated dual-band down tilt omni- directional antennas for 4x4 MIMO with peak antenna gain of 3.5dBi in 2.4GHz and 5.4dBi in 5GHz. Built-in antennas are optimized for horizontal ceiling mounted orientation of the AP. The down tilt angle for maximum gain is roughly 30 degrees.	
1.6.1.25.1.	a mix of horizontally and vertically polarized antenna elements is used.	
1.6.1.25.2.	combining the patterns of each of the antennas of the MIMO radios, the peak gain of the combined, average pattern is 1.9dBi in 2.4GHz and 3.5dBi in 5GHz.	
1.6.1.26.	Must have two (2) multi-gigabit ports (maximum negotiated speed 5Gbps).	
1.6.1.26.1.	auto-sensing link speed (100/1000/2500/5000BASE-T) and MDI/MDX	
1.6.1.26.2.	2.5Gbps and 5Gbps speeds comply with NBase-T and 802.3bz specifications	

1.6.1.26.3.	POE-PD: 48Vdc (nominal) 802.3at/bt POE (class 4 or higher)	
1.6.1.26.4.	802.3az Energy Efficient Ethernet (EEE)	
1.6.1.27.	Must have LACP support between both network ports for redundancy and increased capacity.	
1.6.1.28.	Must have POE power that can be drawn from either port (single source or set to prioritize) or both ports simultaneously (set to combine). (e.g., when set to prioritize, the AP draws power from port1 and may failover to port2).	
1.6.1.29.	Must have DC power interface: 48Vdc (nominal, +/- 5%), accepts 1.35mm/3.5mm center-positive circular plug with 9.5mm length.	
1.6.1.30.	Must have USB 2.0 host interface (Type A connector).	
1.6.1.31.	Must support Bluetooth 5.0 Low Energy (BLE5.0) and Zigbee (802.15.4) radio (2.4GHz).	
1.6.1.32.	Must have visual indicators (two multi-color LEDs): for System and Radio status.	
1.6.1.33.	Must have reset button: factory reset, LED mode control (normal/off).	
1.6.1.34.	Must have serial console interface (micro-B USB physical jack).	
1.6.1.35.	Must have Kensington security slot.	
1.6.1.36.	Must have at least 2.97 Gbps maximum real-world speed (HE80/HE20).	
1.6.1.37.	Must support WPA3 and Enhanced Open security.	
1.6.1.38.	Must have built-in technology that resolves sticky client issues for Wi-Fi 6 and Wi-Fi 5 devices.	
1.6.1.39.	Must support orthogonal frequency-division multiple access (OFDMA) and Multi-User (MU)-MIMO for enhanced MU efficiency.	
1.6.1.40.	Must have IoT-ready Bluetooth 5 and Zigbee support.	
1.6.1.41.	Must be high performance dual radio 802.11ax AP with OFDMA and MU-MIMO.	
1.6.1.42.	Must support maximum data rates of 2.4 Gbps in the 5 GHz band and 1,150 Mbps in the 2.4 GHz band (for an aggregate peak data rate of 3.55 Gbps).	
1.6.1.43.	Must have Bluetooth Low Energy (BLE) and Zigbee radios for location and IOT use cases.	
1.6.1.44.	Must support multi-user transmission with downlink and uplink OFDMA.	
1.6.1.45.	Must support multi-user capability with uplink and downlink MU-MIMO.	

1.6.1.46.	Must have unified AP support which has flexibility to deploy in either controller-based, cloud-managed, or controller-less networks.	
1.6.1.47.	Must support dual radio 802.11ax AP with OFDMA and MU-MIMO:	
1.6.1.47.1.	up to 1024 simultaneous clients per radio	
1.6.1.47.2.	horizontally and vertically polarized antenna elements is used	
1.6.1.47.3.	802.11ax Target Wait Time (TWT) to support low power client devices	
1.6.1.48.	Must have the following support for the multi-gigabit port 1 uplink:	
1.6.1.48.1.	up to 2.5/5 Gbps with NBase-T and IEEE 802.3bz Ethernet compatibility.	
1.6.1.48.2.	backwards compatible with 100/1000Base-T.	
1.6.1.49.	Must have built-in Bluetooth Low-Energy (BLE) and Zigbee radio which enables a wide range of IOT use cases, such as asset tracking and mobile engagement.	
1.6.1.50.	Must have device assurance which uses Trusted Platform Module (TPM) for secure storage of credentials and keys, as well as secure boot.	
1.6.1.51.	Must have Intelligent Power Monitoring (IPM) which enables the AP to continuously monitor and report hardware energy consumption. They can also be configured to enable or disable capabilities based on available PoE power – ideal when wired switches have exhausted their power budget.	
1.6.1.52.	Must have green AP system feature to support a custom deep-sleep mode to deliver significant power and cost savings.	
1.6.2.	WIRELESS ACCESS POINTS FOR EXECUTIVE AND MEETING ROOMS	
1.6.2.1.	The bidder must provide eight (8) units of Wireless Access Point (AP) for Executive and Meeting Rooms with complete accessories and satisfy the minimum requirements and specifications below.	
1.6.2.2.	Must be an indoor AP type with high-end dual radio, 5GHz and 2.4GHz 802.11ax single user MIMO.	
1.6.2.3.	For 5GHz radio: two (2) SS SU-MIMO for up to 1.2Gbps wireless data rate (HE80).	
1.6.2.4.	For 2.4GHz radio: two (2) SS SU-MIMO for up to 287Mbps wireless data rate (HE20).	
1.6.2.5.	Must have three (3) years warranty, support, and subscriptions.	
1.6.2.6.	Must support up to 256 associated client devices per radio, and up to 16 BSSIDs per radio.	
1.6.2.7.	Must support the following frequency bands:	

1.6.2.7.1.	2.400 to 2.4835GHz	
1.6.2.7.2.	5.150 to 5.250GHz	
1.6.2.7.3.	5.250 to 5.350GHz	
1.6.2.7.4.	5.470 to 5.725GHz	
1.6.2.7.5.	5.725 to 5.850GHz	
1.6.2.7.6.	5.850 to 5.895GHz	
1.6.2.8.	Must support the DFS which optimizes the use of available RF spectrum.	
1.6.2.9.	Must support the following radio technologies:	
1.6.2.9.1.	802.11b: DSSS	
1.6.2.9.2.	802.11a/g/n/ac: OFDM	
1.6.2.9.3.	802.11ax: OFDMA with up to eight (8) resource units	
1.6.2.10.	Must support the following modulation types:	
1.6.2.10.1.	802.11b: BPSK, QPSK, CCK	
1.6.2.10.2.	802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM	
1.6.2.10.3.	802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM	
1.6.2.10.4.	802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM	
1.6.2.11.	Must support 802.11n high-throughput support: HT20/40.	
1.6.2.12.	Must support 802.11ac very high throughput support: VHT20/40/80.	
1.6.2.13.	Must support 802.11ax high efficiency support: HE20/40/80/160.	
1.6.2.14.	Must support the following data rates (Mbps):	
1.6.2.14.1.	802.11b: 1, 2, 5.5, 11	
1.6.2.14.2.	802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54	
1.6.2.14.3.	802.11n: 6.5 to 300 (MCS0 to MCS15, HT20 to HT40), 400 with 256-QAM	
1.6.2.14.4.	802.11ac: 6.5 to 867 (MCS0 to MCS9, NSS = 1 to 2, VHT20 to VHT80), 1,083 with 1024-QAM	
1.6.2.14.5.	802.11ax (2.4GHz): 3.6 to 574 (MCS0 to MCS11, NSS = 1 to 2, HE20 to HE40)	
1.6.2.14.6.	802.11ax (5GHz): 3.6 to 1,201 (MCS0 to MCS11, NSS = 1 to 2, HE20 to HE80)	
1.6.2.15.	Must support 802.11n/ac packet aggregation: A-MPDU, A-MSDU.	

1.6.2.16.	Must have transmit power that is configurable in increments of 0.5 dBm.	
1.6.2.17.	Must support the following maximum transmit power:	
1.6.2.17.1.	2.4 GHz band: +20 dBm (17 dBm per chain)	
1.6.2.17.2.	5 GHz band: +21 dBm (18 dBm per chain)	
1.6.2.18.	Must support ACC which minimizes the impact of interference from cellular networks.	
1.6.2.19.	Must support MRC for improved receiver performance.	
1.6.2.20.	Must support CDD/CSD for improved downlink RF performance.	
1.6.2.21.	Must support STBC for increased range and improved reception.	
1.6.2.22.	Must support LDPC for high-efficiency error correction and increased throughput.	
1.6.2.23.	Must support TxBF for increased signal reliability and range.	
1.6.2.24.	Must support 802.11ax TWT to support low-power client devices.	
1.6.2.25.	Two integrated semi-directional antennas for 2x2 MIMO with peak single antenna gain of 5.2dBi in 2.4GHz and 5.4dBi in 5GHz. Built-in antennas are optimized for vertical wall or desk mounted orientation of the AP. Combining the patterns of each of the antennas of the MIMO radios, the peak gain of the combined, average pattern is 3.3dBi in 2.4GHz and 2.9dBi in 5GHz.	
1.6.2.26.	Must have two (2) multi-gigabit ethernet wired network ports.	
1.6.2.26.1.	auto-sensing link speed (100/1000/2500BASE-T) and MDI/MDX	
1.6.2.26.2.	2.5Gbps speed complies with NBase-T and 802.3bz specifications	
1.6.2.26.3.	802.3az Energy Efficient Ethernet (EEE)	
1.6.2.26.4.	POE-PD: 48Vdc (nominal) 802.3af/at/bt POE (class 3, 4 or 6)	
1.6.2.27.	Must have DC power interface: 48Vdc (nominal, +/- 5%), accepts 1.35mm/3.5mm center-positive circular plug with 9.5mm length.	
1.6.2.28.	Must have USB 2.0 host interface (Type A connector).	
1.6.2.29.	Must support Bluetooth 5.0 Low Energy (BLE5.0) and Zigbee (802.15.4) radio (2.4GHz).	
1.6.2.30.	Must have visual indicators (two multi-color LEDs): for System and Radio status.	
1.6.2.31.	Must have reset button: factory reset, LED mode control (normal/off).	
1.6.2.32.	Must have serial console interface (micro-B USB physical jack).	

1.6.2.33.	Must have at least 1.5 Gbps of maximum wireless throughput.	
1.6.2.34.	Must support WPA3 and Enhanced Open security.	
1.6.2.35.	Must have built-in technology that resolves sticky client issues for Wi-Fi 6 and Wi-Fi 5 devices.	
1.6.2.36.	Must support OFDMA for enhanced multi-user efficiency.	
1.6.2.37.	Must have IoT-ready Bluetooth 5 and Zigbee support.	
1.6.2.38.	Must have at least four (4) wired network ports and one (1) smart rate muti-gigabit uplink port.	
1.6.2.39.	Must support maximum data rates of 1.2 Gbps in the 5 GHz band and 287 Mbps in the 2.4 GHz band (for an aggregate peak data rate of 1.5 Gbps).	
1.6.2.40.	Must support multi-user transmission with downlink and uplink OFDMA.	
1.6.2.41.	Must have unified AP support which has flexibility to deploy in either controller-based, cloud-managed, or controller-less networks.	
1.6.2.42.	Must support dual radio 802.11ax AP with OFDMA:	
1.6.2.42.1.	provides connectivity for a maximum of 256 associated clients per radio (512 in total)	
1.6.2.42.2.	built-in antennas are optimized for vertical wall or desk mounted orientation of the AP	
1.6.2.42.3.	802.11ax TWT to support low power client devices	
1.6.2.43.	Must have the following support for the multi-gigabit port 1 uplink:	
1.6.2.43.1.	auto-sensing link speed (10/100/1000BASE-T) and MDI/MDX	
1.6.2.43.2.	802.3az Energy Efficient Ethernet (EEE)	
1.6.2.44.	Must have built-in filtering to allow Wi-Fi and BLE/ Zigbee radios to operate at maximum capacity without the impact of interference.	
1.6.2.45.	Must have device assurance which uses TPM for secure storage of credentials and keys, as well as secure boot.	
1.6.2.46.	Must have IPM which enables the AP to continuously monitor and report hardware energy consumption. They can also be configured to enable or disable capabilities based on available PoE power – ideal when wired switches have exhausted their power budget.	
1.6.2.47.	Must have green AP system feature to support a custom deep-sleep mode to deliver significant power and cost savings.	
1.7.	CENTRAL MANAGEMENT SOLUTION FOR NETWORK EQUIPMENT OF EXTENSION OFFICE	

1.7.1.	The bidder must provide one (1) lot cloud-based Central Management Solution for the proposed two (2) units of Core Switch (CS), one (1) unit of Multi-Gigabit PoE Access Switch (MGPAS), four (4) units of Power over Ethernet (PoE) Access Switch (PAS), six (6) units of Wireless Access Point (AP) for the Workforce Area, and eight (8) units of Wireless Access Point (AP) for Executive and Meeting Rooms with minimum requirements and specifications below.	
1.7.2.	Must have three (3) years warranty, support, and subscriptions.	
1.7.3.	Must have unified management of wireless, wired, VPN, and SD-WAN for simplified operations.	
1.7.4.	Must have Artificial intelligence (AI)-based network insights for faster troubleshooting and continuous network optimization.	
1.7.5.	Must have multivendor and third-party integration to proactively monitor and improve the end-user experience.	
1.7.6.	Must have network fabric orchestration, intent-based policy engine, and access controls for unified policy management, automated network provisioning, and zero-trust security.	
1.7.7.	Must have AI-based client insights that enables inline client profiling and telemetry to close visibility gaps associated with IoT.	
1.7.8.	Must have powerful monitoring and troubleshooting for remote or home office networks.	
1.7.9.	Must have APIs and webhooks to augment the value of other leading IT platforms in your environment.	
1.7.10.	Must have live chat and an AI-based search engine for an enhanced support experience.	
1.7.11.	Must have SaaS, on-premises, and Virtual Private Cloud managed service options for flexible consumption and financing.	
1.7.12.	Must have the following Monitoring requirements:	
1.7.12.1.	Network health and assurance – gain broad visibility into network-wide performance, and drill-in to specific sites with summaries of device utilization, configuration compliance, and other statistics.	
1.7.12.2.	Application visibility – monitor application health across the network, ensuring critical services receive priority traffic while tracking and enforcing acceptable usage by site, device, or location.	
1.7.12.3.	Unified Communication and Collaboration (UCC) Analytics – a consolidated view of how VoIP applications are performing display's mean opinion scores, and potential RF performance and capacity issues.	
1.7.12.4.	Additional visibility into key values of individual and stacked switches is provided. This includes port status, PoE consumption, VLAN assignment, device and neighbor	

	connections, power status and trends, alerts, and events and which troubleshooting actions can be performed.	
1.7.13.	Must have the following Management and Troubleshooting requirements:	
1.7.13.1.	When a network- or business-impacting problem occurs, quick detection, root cause identification, and resolution are at the core of maintaining a stable environment – enables 24x7, intelligent monitoring of networks, applications, client devices, and end-user experience, all correlated into powerful visualizations and dashboards.	
1.7.13.2.	Network Insights – automatically surface and diagnose an array of common network-impacting issues by using dynamic, per-site baselines that are continuously tuned as conditions change; no manual setup or adjustment of service level thresholds required. Built-in anomaly detection highlights the severity and impact of issues as they occur, helping administrators pinpoint root cause and proper remediation steps with 95% accuracy.	
1.7.13.3.	AI Search – a language processing engine points to solution guides, troubleshooting tips, and more. Whether operators are looking for best practices on device configurations or need to isolate a problem impacting a specific user, AI Search provides fast, interactive responses that simplify Day 0 to Day 2 operations.	
1.7.13.4.	AI Assist – uses event-driven automation to collect diagnostics for critical failure signatures for proactive customer support and replacement workflows.	
1.7.13.5.	AI-powered Client Insights – granular visibility and profiling of clients with up to 99% accuracy by using native telemetry from infrastructure without the installation of physical collectors or agents. Deep packet inspection that uses client and device attributes coupled with machine learning models are used to fingerprint, identify, and accurately profile a wide variety of clients across the entire wired and wireless infrastructure. This approach reduces deployment time and cost and accelerates time-to-value while increasing visibility and security posture.	
1.7.13.6.	Built-in Troubleshooting Tools – troubleshooting capabilities include live events, which provide details such as occurrence time, device name, device type, category, and description. Additionally, packet capture, logs, and rich command line tools are included for troubleshooting.	
1.7.14.	Must have the following Security requirements:	
1.7.14.1.	AI-based Client Profiling	
1.7.14.2.	Eliminate Indoor Cellular Gaps	
1.7.14.3.	User and Device Authentication	
1.7.14.4.	Simplified and Efficient Operations	

1.7.14.5.	Global policy automation and orchestration	
1.7.14.6.	Flexible Technology Eases Migration	
1.7.14.7.	Secure Wireless Segmentation	
1.7.14.8.	Intrusion Detection	
1.7.14.9.	Web Content Filtering	
BUDGET REQUIREMENTS		
2.1.	The budget for One (1) Lot Supply, Delivery, Installation, Configuration, Implementation, Commissioning, and Support Services for the Enhancement of GCG Main and Extension Office Network Infrastructure is Fourteen Million Seven Hundred Fifty Thousand Pesos Only (₱14,750,000.00).	
BIDDER REQUIREMENTS		
3.1.	General Requirements	
3.1.1.	The bidder must provide the following documents during the post-qualification:	
3.1.1.1.	a certification issued by the product manufacturer that they are a certified partner and able to extend direct technical support to end-user for each product brand being offered; and	
3.1.1.2.	copy of company's latest General Information Sheet (GIS).	
3.1.2.	The bidder must have at least five (5) years of continuous existence and engagement in the IT business.	
3.1.3.	The bidder must have completed a similar contract for the supply, delivery, and installation of firewall and network infrastructure for the past three (3) years from the date of submission and receipt of bids.	
3.1.4.	The bidder must be a Platinum PhilGEPS registered supplier.	
3.1.5.	Subcontractors are prohibited.	
3.2.	Manpower Requirements	
3.2.1.	The bidder must provide a list of locally based manpower for the supply, delivery, installation, configuration, and commissioning of the proposed enhancement of the network infrastructure for the Main Office and Extension Office of the GCG, with each personnel being a regular employee **either** of the bidder, **bidder's product distributor, or bidder's product principal**:	
3.2.1.1.	one (1) Certified Network Associate or equivalent;	
3.2.1.2.	one (1) Certified Network Professional or equivalent; and	
3.2.1.3.	one (1) Certified Accredited Engineer of the proposed NGFW.	

3.2.2.	The bidder must provide a photocopy of valid certifications, resume, and company ID of the identified local manpower during post-qualification.	
3.2.3	**Prior to submission of bid, the prospective bidder is required to conduct an ocular inspection of the GCG extension office located at 17th Floor BDO Towers Valero, Valero Street, Makati City. The purpose of this inspection is to allow the bidder to be familiarized with the conditions and requirements for the feasibility of the project.**	
3.2.3.1	**The schedule date and time for the ocular inspection will be on 07 March 2024 from 10:00 AM until 12:00 PM.**	
3.2.3.2	**Attendance at the ocular inspection is mandatory for all prospective bidders. Failure to attend the ocular inspection will result in disqualification from the bidding process.**	
3.2.3.3	**The bidder must send an email request to the GCG at procurement@gcg.gov.ph on or before 06 March 2024 02:00PM to confirm their participation in the mandatory ocular inspection. The email must contain the company name and the names of bidder representatives (maximum of 2). This is to secure in advance the required gate pass and permit to enter the office building prior to the scheduled date of ocular inspection.**	
3.2.3.4	**The bidder must obtain a Certificate of Appearance as proof of their attendance at the ocular inspection. The certificate shall be issued by the designated representative of the GCG present during the inspection.**	
3.2.3.5	**The Certificate of Appearance must be included in the bidder's submission along with the bid documents. Bids submitted without the Certificate of Appearance will be considered as non-compliant.**	
3.2.3.6	**The GCG reserves the right to verify the accuracy of the information provided in the Certificate of Appearance. Any falsification of attendance will result in disqualification and other appropriate actions.**	
SCOPE OF WORK		
The Winning Bidder (hereafter referred to as simply the "bidder") must:		
4.1.	Perform the supply, delivery, installation, configuration, implementation, commission, and support services of the proposed enhancement of network infrastructure for the GCG's Main Office at 3rd Floor BDO Towers Paseo (formerly Citibank Center) 8741 Paseo de Roxas, Makati City, and GCG Extension Office at 17th Floor BDO Towers Valero, Valero Street, Makati City.	

4.2.	Cover all cables, structured cabling, civil works, licenses and/or subscriptions needed for the implementation of the proposed enhancement of GCG Main and Extension Office network infrastructure, including, but not limited to the following:	
4.2.1.	install, configure, and implement the proposed one (1) unit of External Firewall Central Management Solution with complete integration to the existing two (2) units of External Firewalls in the GCG Main Office (Palo Alto 3220);	
4.2.2.	install, configure, and implement the proposed two (2) units of Next Generation Firewalls for the GCG Extension Office with complete integration to the proposed External Firewall Central Management Solution for the GCG Main Office;	
4.2.3.	install, configure, and implement the proposed two (2) units of Core Switches for the GCG Extension Office with complete integration to its proposed Next Generation Firewalls;	
4.2.4.	install, configure, and implement the proposed four (4) units of PoE Access Switch for the GCG Extension Office with complete integration to its proposed Core Switches;	
4.2.5.	install, configure, and implement the proposed one (1) unit of Multi-Gigabit PoE Access Switch for the GCG Extension Office with complete integration to its proposed Core Switches;	
4.2.6.	install, configure, and implement the proposed six (6) units of Wireless Access Points for the Workforce Area of the GCG Extension Office with complete integration to its proposed Multi-Gigabit PoE Access Switch;	
4.2.7.	install, configure, and implement the proposed eight (8) units of Wireless Access Points for Executive and Meeting Rooms of the GCG Extension Office with complete integration to its proposed Multi-Gigabit PoE Access Switch through the following deployments:	
4.2.7.1.	one (1) unit must be deployed as desk mounted; and	
4.2.7.2.	seven (7) units must be deployed as wall mounted.	
4.2.8.	install the horizontal cabling distribution needed for the deployment of the new network equipment in the GCG Extension Office;	
4.3.	Conduct Project Management using the below framework:	
4.3.1.	create a project team for the GCG and the bidder;	
4.3.2.	formulate project implementation plan;	
4.3.3.	conduct project kick-off;	
4.3.4.	implement and coordinate project milestones identified in the project implementation plan;	
4.3.5.	provide weekly/monthly/milestone project updates;	

4.3.6.	conduct hands-on technical training on the supplied equipment; and	
4.3.7.	provide and execute user acceptance and test plans.	
4.4.	Submit detailed project documentation in hard and soft copies:	
4.4.1.	Project Implementation Plan;	
4.4.2.	As built drawing;	
4.4.3.	Technical Reports;	
4.4.4.	UAT Test Plan;	
4.4.5.	Service Level Agreement; and	
4.4.6.	Warranty Agreement.	
TRAINING REQUIREMENTS		
5.1.	The bidder shall provide in-depth knowledge transfer on product installation, configuration, administration, maintenance, management, and operation of each proposed equipment for the enhancement of GCG Main and Extension Office network infrastructure to be conducted by a designated product expert.	
WARRANTY, MAINTENANCE, AND SUPPORT		
6.1.	The bidder must warrant that the Goods supplied are brand-new, unused, of the most recent or current models, and that they incorporate all recent improvements in design and materials, except when the technical specifications required by the GCG provides otherwise.	
6.2.	The bidder must further warrant that all Goods supplied shall have no defect, arising from design, materials, or workmanship or from any act or omission of the bidder that may develop under normal use of the supplied Goods.	
6.3.	To ensure that manufacturing defects shall be corrected by the bidder, warranty, support services, and required subscriptions for all equipment and solutions shall be required from the bidder for a minimum period of three (3) years.	
6.4.	The GCG shall promptly notify the bidder in writing of any claims arising under this warranty. Upon receipt of such notice, the bidder shall, within the period specified and with all reasonable speed, repair or replace the defective Goods or parts thereof, without cost to the GCG.	
6.5.	If the bidder, having been notified, fails to remedy the defect(s) within the period specified, the GCG may proceed to take such remedial action as may be necessary, at the bidder's risk and expense and without prejudice to any other rights which the GCG may have against the bidder under the Contract and under the applicable laws.	

6.6.	In the event of any equipment failure, the bidder shall repair or automatically replace the defective products with the same product at no additional cost/charge to GCG.	
6.7.	A functional and workable service unit that is equivalent or higher in specification should be provided in case replacement of hardware would take more than twenty-four (24) hours or if repair requires pull out the equipment from GCG premises.	
6.8.	The bidder must provide a signed after sales service support certificate that the bidder will be supported by their principal in terms of parts and services.	
6.9.	The bidder must provide full-time support and managed services, without additional cost to the GCG, during the warranty period as specified:	
6.9.1.	single point of contact for all hardware and software components;	
6.9.2.	twenty-four hours by seven days (24x7) service desk support via telephone, email, or online chat portal;	
6.9.3.	at least one (1) hour response time upon receipt of issue escalation and four (4) hours for onsite support, if necessary;	
6.9.4.	if the problem was not resolved by service desk support, the bidder must provide an onsite technical support;	
6.9.5.	procedures on support and issue escalation; and	
6.9.6.	service report every after the onsite support.	
TERMS OF PAYMENT		
7.1.	Payments shall be made only upon deployment completion of each item and a certification by the Chairperson or Authorized Representative of the GCG to the effect that the goods delivered is in accordance with this Terms of Reference (TOR) and have been duly accepted. Except with the prior approval of the Chairperson of the GCG, no payment shall be made for supplies and materials not yet delivered under this TOR.	
7.2.	Provided further that payment shall be made within twenty (20) working days from the receipt of complete documents, i.e., billing statement / statement of account, and other pertinent documents from the bidder.	
7.3.	All payments made to the bidder will be subjected to a five percent (5%) reduction, to serve as retention money. The said amounts shall only be released after the lapse of the warranty period.	
CONFIDENTIALITY		
8.1.	Information or rights acquired and obtained from the GCG, including but not limited to any and all obligations prior to the termination or expiration hereof and provisions on confidentiality and proprietary rights, will remain in effect after termination of the services rendered to the GCG. Hence, the undertaking of the bidder not to disclose and to keep information confidential shall subsist even after the	

	expiration or termination of its obligation to the GCG nor can the bidder, at any time, disclose items mentioned or enumerated in Section 8.2 or any information it acquires by virtue of the contract which the GCG deems confidential.	
8.2.	Records, documents, reports, and relevant data, such as diagrams, plans, designs, estimates, specifications, and other supporting records of materials complied and prepared in the courses of the performance of the services shall be absolute properties of GCG and shall not be used by the bidder for purposes not related to this agreement without prior written approval of GCG. Copies of such documents as required in this TOR shall be turned over to GCG upon completion of the project except that the bidder shall have the right to retain a copy of the same.	
DELIVERY AND IMPLEMENTATION SCHEDULE		
9.1.	The delivery of goods, project implementation, documentation, and acceptance must be completed within one hundred eighty (180) calendar days from the receipt of the Notice to Proceed.	
9.2.	The bidder shall be subjected to evaluation by the end-user after the implementation of the project.	