

INVITATION TO BID FOR THE

**Supply, Delivery, Installation, and Configuration of Next Generation Firewall Appliance and Internet Dedicated Service (IDS), and related services for the Philippine Tax Academy (PTA)
Public Bidding No. 23-08-2**

The **Philippine Tax Academy (PTA)**, through its **Corporate Operating Budget FY 2023** intends to apply the sum of **Twenty Million Nine Hundred Thousand Pesos (Php 20,900,000.00)** being the ABC to payments under the contract for **Supply, Delivery, Installation, and Configuration of Next Generation Firewall Appliance and Internet Dedicated Service (IDS) and related services for the Philippine Tax Academy (PTA)**

1.

Lot No.	Quantity	Item/Description	Approved Budget for the Contract	Price of Bid Documents
1	1 lot	Next Generation Firewall Appliance	₱ 5,100,000.00	₱ 10,000.00
2	1 lot	High Availability (HA) Network Solution	₱ 8,000,000.00	₱ 15,000.00
		Internet Dedicated Services with High Availability	₱ 5,000,000.00	
		Managed Service - PABX System	₱ 1,500,000.00	
		Wireless Access Points with Cloud-based Management and Administration	₱ 800,000.00	
		Structured Cabling - Voice and Data	₱ 500,000.00	
			₱ 15,800,000.00	
Total:			₱ 20,900,000.00	₱ 25,000.00

Bids received in excess of the ABC shall be automatically rejected at bid opening.

2. The **PTA**, through its Bids and Awards Committee (BAC), now invites bids for the above Procurement Project. Delivery of the Goods is required by **Lot 1: Sixty (60) calendar days upon receipt of Notice to Proceed and Lot 2: Sixty (60) calendar days upon receipt of Notice to Proceed**. Bidders should have completed, within *five (5) years* from the date of submission and receipt of bids, a contract similar to the Project. The description of an eligible bidder is contained in the Bidding Documents, particularly, in Section II (Instructions to Bidders).

Summary of the bidding activities is as follows:

Advertisement/Posting of Invitation to Bid	Friday, 18 August 2023
Issuance and Availability of Bid Documents	Friday, 18 August 2023
Pre-Bid Conference	Tuesday, 29 August 2023; 10:00AM
Last Day of Request for Clarification	Friday, 01 September 2023
Last Day for Issuance of Supplemental Bid Bulletin	Tuesday, 05 September 2023
Deadline for Submission of Bids	Tuesday, 12 September 2023;10:00AM
Opening of Bids	Immediately after the Deadline for Submission of Bids

3. Bidding will be conducted through open competitive bidding procedures using a non-discretionary “*pass/fail*” criterion as specified in the 2016 revised Implementing Rules and Regulations (IRR) of Republic Act (RA) No. 9184, otherwise known as the “Government Procurement Reform Act”.

Bidding is restricted to Filipino citizens/sole proprietorships, partnerships, or organizations with at least sixty percent (60%) interest or outstanding capital stock belonging to citizens of the Philippines, and to citizens or organizations of a country the laws or regulations of which grant similar rights or privileges to Filipino citizens, pursuant to RA No. 5183 and subject to Commonwealth Act 138.
4. Interested Bidders may obtain further information from the Office of the PTA and inspect the Bidding Documents through the Bids and Awards Committee (BAC) Secretariat at the address given below during 8:00 am to 5:00 pm.
5. A complete set of Bidding Documents may be acquired by interested Bidders on **18 August 2023** from the given address and website(s) below and upon payment of the applicable fee for the Bidding Documents, pursuant to the latest Guidelines issued by the GPPB, in the following amount **Lot 1: Ten Thousand Pesos (₱ 10,000.00) and Lot 2: Fifteen Thousand Pesos (₱ 15,000.00)**. The Procuring Entity shall allow the bidder to present its proof of payment for the fees in person or through electronic means.
6. The PTA will hold a Pre-Bid Conference on **29 August 2023 at 10:00 a.m.** at the **3rd Floor DOF Conference Room, DOF Building** or through video conferencing or webcasting via Google Meet which can be accessed thru this link: and shall be open to **meet.google.com/cdg-tqpc-ddr** prospective bidders.
7. Bids must be duly received by the BAC Secretariat through manual submission at the Ground Floor, DOF Bldg., BSP Complex, Roxas Blvd., Malate, Manila, on or before **12 September 2023 at 10:00 a.m.**

Late bids shall not be accepted. Unsealed or unmarked bid envelopes shall also be rejected.
8. All Bids must be accompanied by a bid security in any of the acceptable forms and in the amount stated in **ITB** Clause 14.
9. Bid opening shall be on **12 September 2023 at 10:00 am** at the 3rd Floor DOF Conference Room, DOF Building. Bids will be opened in the presence of the bidders’

representatives who choose to attend the activity.

10. Bidders shall drop their duly accomplished eligibility requirements, technical and financial proposals in two separate sealed envelopes in the designated bid box located at the at the Ground Floor, DOF Bldg., BSP Complex, Roxas Blvd., Malate, Manila.
11. The **PTA-BAC** reserves the right to reject any and all bids, declare a failure of bidding, or not award the contract at any time prior to contract award in accordance with Sections 35.6 and 41 of the 2016 revised IRR of RA No. 9184, without thereby incurring any liability to the affected bidder or bidders.
12. For further information, please refer to:

LEEANN Q. BAUTISTA
Bids and Awards Committee Secretariat
Philippine Tax Academy
7th Floor EDC Building,
BSP Complex, Roxas Boulevard
Malate, Manila
Email: bacsec@doftaxacademy.gov.ph
Contact Number: 5317-6363 local 6200
13. You may visit the following websites:

For downloading of Bidding Documents:
<https://doftaxacademy.gov.ph>
<https://notices.philgeps.gov.ph/>

15 August 2023


ATTY. NOEMI B. ALCALA-GARCIA
BAC Chairperson

TERMS OF REFERENCE

PROJECT TITLE: Next Generation Security Firewall Appliance

SCHEDULE OF REQUIREMENTS:

Description	Quantity	Delivery Schedule
Next Generation Firewall Appliance with Three (3) year Warranty on Hardware Appliance, Licenses and Support Services.	1 lot	Sixty (60) Calendar days upon receipt of Notice to Proceed
Configuration, Implementation and installation Services		
Knowledge Transfer Training		

ABC: 5.1M

SCOPE OF WORK: Supply, delivery, installation and configuration of Next Generation Firewall Appliance (NGFW).

The deployment task includes the following:

1. Project Kick-Off
2. The winning bidder will provide Network Topology Design and Documentation.
3. The winning bidder will perform the following tasks to install and configure a Next-Generation Firewall:
 - 3.1. Installation of NGFW Appliance in PTA's network environment (includes mounting to PTA rack, power supply, and fan trays if applicable.)
 - 3.2. Update NGFW to latest firmware, and activate licenses support and subscription (Advance Threat Prevention, DNS Security, Advance URL Filtering, Advance Threat Analysis, etc.)
 - 3.3. Configure Firewall policies, NAT configuration, Zones, Routes, Services, Objects, VLANs, IP addresses, interfaces, and test basic routing capabilities.
 - 3.4. Configure WAN connectivity, WAN Failover, SSL Decryption, SSL VPN, IPsec VPN(Site to site) and syslog.
 - 3.5. Perform functionality testing of internal and external application/servers.
 - 3.6. Prevent customer's server and user for attacks and Intrusion
 - 3.7. Assess and review the routes for each network traffic
 - 3.8. Discover business needs for network and security distribution
 - 3.9. Burn-test NGFW Appliance for 24 hours.
4. Activate licenses support and subscription features (URL Filtering, Threat Prevention, and Wildfire)

5. The winning bidder will implement User-ID or IP-Base security function in the PTA Domain as defined in the design documentation.
6. The winning bidder will provide User-ID to IP mapping. Tasks will include:
 - 6.1. Map User-ID to IP address information for the number of Authentication domains as defined in the design.
 - 6.2. Collect User Group information per defined authentication domain.
 - 6.3. Requirements review and definition of User domain environments.
 - 6.4. Use of system logs to gather User and IP address information.
7. The winning bidder will implement App-ID functionality in the Targeted Network/Policy.
 - 7.1. Convert all well-known applications from Port-based rules to application-based policies.
 - 7.2. Isolate all unknown TCP/UDP traffic rules.
 - 7.3. Finalize and modify App-ID policy on a third scan performed at agreed scheduled time, subsequent to completion of the second App-ID scan.
 - 7.4. Remove Port-based rules.
8. The winning bidder will configure Advance URL Filtering on Next Generation Firewall Network Perimeter Device:
 - 8.1. Manually convert existing Content Filtering rules to Advance URL Filtering profile.
 - 8.2. Block agreed high risk categories.
 - 8.3. Review with PTA - DOF existing URL Filtering rules and determine necessary parameters for mapping into Next Generation Firewall Networks URL Filtering categories.
 - 8.4. Manually convert an existing URL Content service to NGFW Advance URL Filtering
 - 8.5. Create and implement a Next Generation Firewall Advance URL Filtering policy.
9. Knowledge Transfer Training
The winning bidder will provide trainings to PTA technical team on the deployed NGFW. The handover process will covers the installation, configuration, and administration of the NGFW solution.
10. The winning bidder must provide as-built plan documentation.
11. The winning bidder must provide semi-annual Health Check Maintenance with the following as part of a health check service:
 - 11.1. Current patch levels.
 - 11.2. Identification of any performance issues.
 - 11.3. Identification of any potential security issues.
 - 11.4. Identification of any potential server (hardware) issues.

TECHNICAL SPECIFICATIONS:

1. Hardware Specifications

- 1.1. The proposed Next Generation Firewall must support the following:
 - Not lower than 6.8 Gbps of Firewall Throughput.

- Nine hundred forty-five thousand 945,000 maximum sessions and at least One hundred thousand 100,000 new sessions per second.
- Not lower than 3.2 Gbps of Threat Prevention throughput.
- Not lower than 4.6 Gbps of Internet Protocol Security (IPSEC) Virtual Private Network (VPN) throughput.
- 12 x RJ-45 10/100/1000Mbps ports for network traffic.
- High-Availability (HA) both Active/Active and Active/Passive modes.
- Fully redundant power supply with an additional power supply module
- Not lower than 120 GB SSD disk drive capacity.

2. Functional Requirements

- 2.1. The Proposed Next-Generation Firewall must have a separate and dedicated CPU, Memory, and Hard drive for the control plane and data plane. To avoid service interruption on the data processing plane when the control plane has been restarted or rebooted.
- 2.2. A hardened Operating System (OS) must be built as a firewall appliance and not built from generic server hardware.
- 2.3. Must handle all traffic in a single pass stream-based manner with all security features turned on to deliver predictable performance. It shall be optimized for Layer Seven (7) application-level content processing to handle signature matching and processing in a single-pass parallel processing architecture.
- 2.4. Must have a basic malware analysis service without any additional subscription. The firewall should forward portable executable files to the malware analysis service for analysis
- 2.5. Must offer safe application enablement capabilities to build firewall policies based on application/application features, users and groups, and content, as opposed to port, protocol, and IP address, transforming your traditional allow or deny firewall policy into business-friendly elements.
- 2.6. Must support application detection, which determines what an application is irrespective of port, protocol, encryption Secure Shell or Secure Sockets Layer (SSH or SSL), or any other evasive tactic the application uses. The solution must support multiple classification mechanisms such as application signatures, application protocol decoding, and heuristics to your network traffic stream to accurately identify applications
- 2.7. Must support dynamic addition of workload into a dynamic address object. Any additional workload into a pool of servers belonging to a dynamic address object will automatically apply the corresponding security policy without manual intervention.
- 2.8. Must natively support decryption of Transport Layer Security (TLS) 1.3 without downgrading to TLS 1.2

- 2.9. Must provide enhanced reporting and logging of decrypted and encrypted traffic.
 - 2.10. Must be able to integrate to an external web server Hypertext Transfer Protocol Secure (HTTP/S) containing dynamic IP, Uniform Resource Locators (URL), or Domain list(s) that can be referenced for security policy (e.g., whitelisting or blacklisting purposes). Any changes on the list should be dynamically captured and automatically applied to the security policy without manual intervention.
 - 2.11. It must have an interactive and customizable graphical summary of the applications, users, URLs, threats, and content traversing the network it protects.
 - 2.12. Must provide a unified view of logs and separate detailed logs for each type (e.g., traffic, URL, threats, file analysis, system, configuration, users, etc.) for easy analysis.
 - 2.13. Must be able to natively trigger custom alerts/logs based on conditions produced by different event sources (e.g., traffic, threat, URL, system, configuration) and forward customizable attribute value via HTTP-based service that exposes an Application Programming Interface (API) (via HTTPS), email Simple Mail Transfer Protocol (SMTP), Syslog and Simple Network Management Protocol (SNMP) Trap.
 - 2.14. Must have native built-in functionality to auto quarantine or blacklist IP addresses to existing security policies based on any log attributes from multiple log sources (e.g., traffic, threat, URL, etc.).
- 3. Certification / Accreditation / Awards**
- 3.1. The proposed solution must be in the leader's quadrant position of Gartner Magic Quadrant for Enterprise Network Firewall. (Must be verifiable thru Gartner's Website)
 - 3.2. The proposed solution must be from a security vendor that is part of the leader category in the Forrester Wave Zero Trust extended Ecosystem Platform Providers to support PTA towards a Zero Trust framework. (Must be verifiable thru Forrester's Website or Principal's website)
 - 3.3. The cloud-based malware analysis platform of the proposed solution must have SOC2 Type II Plus certification. (Must be verifiable thru Principal's website).
- 4. Local Management**
- 4.1. The proposed Next Generation Firewall must be fully configurable and manageable using a Web-based Graphical User Interface (GUI) via a standard Web Browser (HTTP) and/or Command Line Interface (CLI) via Secure Shell (SSH) application. No additional client software shall be required to configure security policies, objects, etc.
 - 4.2. The proposed solution, if managed by a Central Management System, must be able to add, edit or remove firewall policies that are

locally created. The FW appliance will allow flexibility when the Central Management System (CMS) is down/unreachable or security policies are applicable only to specific Virtual Next Generation Security Firewalls.

- 4.3. Must generate local reports on a manual ad-hoc or schedule (daily, weekly, monthly, etc.) without additional software subscription/licenses or hardware components.
- 4.4. Must log all administrative activities on the web and the command line interface.
- 4.5. Must be able to assign management functions for each user or group granularly defined Role Based Access Control (RBAC).
- 4.6. Must support Extensible Markup Language (XML) Application Programming Interface (API) that allows other systems to manage/integrate with the solution.
- 4.7. Must have a native policy optimization tool to help effectively migrate from traditional/legacy port protocol to application-based rules. It must have usage tracking of the actual application for every security policy that utilizes Port Based Rules (PBR).
- 4.8. Must have a native policy optimization tool that can help identify unused security policies. It must not be limited to policy hit count and must have policy rule usage analysis based on an adjustable time frame.
- 4.9. Must have a native policy optimization tool to help track and fix overly permissive security policies (allow any port/application).
- 4.10. Must have tagging or labeling capability attached to security policies and objects for automation and policy management optimization.
- 4.11. It must have a global search function that allows the security admins to search for policy names and objects across your entire configuration.

5. Threat Prevention

- 5.1. The proposed solution must inspect all traffic for threats, regardless of port and protocol, and automatically blocks known vulnerabilities, malware, exploits, spyware, and Command-and-Control (C&C).
- 5.2. For the encrypted traffic Secure Socket Layer (SSL), the proposed solution must be able to selectively apply a policy-based decryption and then inspect the traffic for threats, regardless of ports.
- 5.3. 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.
- 5.4. The security platform must support an external dynamic list where it offers the capability to ingest multiple feeds from third-party Indicators of Compromise (IOCs) feeds on IP addresses, URLs, or Domains, then can be automated into policy enforcement to deny/reset/drop the matching traffic. If yes, please provide evidence to support the statement.

- 5.5. Must support packet capturing of specific threats for forensic evidence or investigation.
 - 5.6. It must provide the ability to allow the organization to write its customized threat signatures for new or targeted threats that may not be found in other environments.
 - 5.7. Must be able to define different antivirus/vulnerability protection / antispyware security profiles for each security policy defined.
- 6. Domain Name System (DNS) Security**
- 6.1. The proposed solution must stop known and unknown DNS traffic with Machine Learning (ML) and predictive analytics.
 - 6.2. Must help identify systems that are infected/compromised by sink holing DNS requests to a command and control server
 - 6.3. 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 C&C server. In addition, it should identify DGA domains based on dictionary words.
 - 6.4. Protect against DNS Tunneling-based attacks that utilize crafted DNS queries and responses to hide malware delivery, C&C traffic, or data exfiltration/extraction.
 - 6.5. Must protect against ultra-low/slow DNS tunnels that spread tunneled data and exploits across multiple domains and use prolonged rates to evade detection, steal data, or send additional malicious payloads into your network.
 - 6.6. Must protect against strategically aged domains using predictive analytics. It should protect users from connecting to reserved domains and left dormant for months before use by malicious actors.
 - 6.7. It must prevent fast flux, a technique cybercriminals use to cycle through bots and DNS records. Fast flux networks are used for phishing, malware distribution, scams, and botnet operations.
 - 6.8. Must protect against domains surreptitiously added to hacked DNS zones of reputable domains.
 - 6.9. Must prevent DNS rebinding attacks, which can be used to move laterally and attack services inside the corporate network from the internet.
 - 6.10. Must prevent dangling DNS attacks, which use stale DNS zone data to take over domains and cause reputational harm or launch phishing attacks.
 - 6.11. Must support the following DNS Security Categories:
 - Command and Control (C2) or (C&C)
 - Dynamic DNS (DDNS)
 - Malware
 - Newly Registered Domains
 - Phishing
 - Grayware
 - Parked
 - Proxy Avoidance & Anonymizers

7. **Advanced Uniform Resource Locators (URL) Filtering**
- 7.1. Must have natively-integrated URL filtering capabilities.
 - 7.2. Must support locally defined URL entries/categories.
 - 7.3. Must have an automated cloud-based dynamic URL categorization for classifying unknown websites.
 - 7.4. Must have a specific category for Malware, Phishing, Command-and-Control, Proxy Avoidance, and Anonymizers, among other usual web categories.
 - 7.5. Must support multi-category URL filtering capabilities that include risk categories for more granular URL categorization.
 - 7.6. Must have Inline (Machine Learning) 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).
 - 7.7. 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 (CAPTCHAs), and Hypertext Markup Language (HTML) character encoding.
 - 7.8. Must have real-time detection and prevention of credential theft by controlling sites where users can submit corporate credentials based on the site's URL category.
 - 7.9. Must have phishing image detection that uses ML models to analyze images on web pages to determine whether they are imitating brands commonly used in phishing attempts.
 - 7.10. 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).
 - Except for government, banking institution, and healthcare provider URL categories from decryption.
8. **Advanced Threat Analysis**
- 8.1. The proposed solution must identify unknown malware using a cloud-based malware analysis platform with advanced detection capabilities like Static & Dynamic Analysis, Bare-metal analysis, Machine Learning, Dynamic unpacking, Network Traffic profiling, and Recursive Analysis.
 - 8.2. The proposed cloud-based malware analysis platform must have Security Operations Center (SOC)2 Type II Plus Certification.
 - 8.3. Must support automatic creation and delivery of protection signatures from locally submitted samples and dynamic updates from the platform.
 - 8.4. The proposed cloud-based malware analysis platform must have a custom-built hypervisor that detects and analyze evasive attacks.

- 8.5. Must be able to identify and prevent variants of known malware Portable Executable (PE and PowerShell file types) in real-time using the local machine learning module.
 - 8.6. Must have a machine learning module that is updated automatically in the form of training sets from the cloud-based advanced malware analysis platform.
- 9. Warranty, Support and Service Level Agreement (SLA)**
- 9.1. The proposed solution must include 3 Years Warranty on the following Licenses, Appliance, and Support services:
 - Hardware Appliance
 - Advance Threat Prevention
 - DNS Security
 - Advance URL Filtering
 - Advance Wildfire Protection
 - SDWAN
 - 9.2. Service Level Agreement SLA
 - 24x7 Helpdesk Support
 - 8x5xnb (next business day) with parts and onsite service support for appliance and configurations during the warranty period.
 - Must provide service unit in case of appliance failure or errors within 48 hours from when the incident is reported.
- 10. Additional Requirements**
- 10.1. The Supplier must have at least two (2) Certified Network Security Engineer of the proposed solution and must be employed in the company for at least 2 years. (must provide copy of Engineers Certification from the manufacturer and Certificate of Employment, Company – ID, and Resume/CV).
 - 10.2. The Supplier must submit Manufacturer/Principal Authorization Certification of the proposed Solution.
 - 10.3. The Supplier must be at least twenty (20) years in the IT Industry.

TERMS OF REFERENCE

SCHEDULE OF REQUIREMENTS

Item No.	Item Description	Contract Duration	Delivery Period	ABC
# 1	<p>Internet Dedicated Service with High-Availability (IDS-HA)</p> <p>a.) Independent ISP 1 - 150 Mbps IDS Connection speed with modem/media converter.</p> <p>b.) Independent ISP 2 - 150 Mbps IDS Connection speed with modem/media converter.</p> <p>c.) Two (2) Managed Router that can accommodate up to 200 Mbps traffic throughput</p> <p>d.) One (1) Managed Service Load Balancer Internet Access Gateway Appliance</p>	One (1) year upon the Issuance of the Certificate of Operationality	Delivery, Configuration, and Installation service shall be completed within sixty (60) calendar days from the issuance of the Notice to Proceed	P 5 Million
# 2	<p>Managed Service PABX System</p> <p>a) One (1) ISDN Port 30 Channels</p> <p>b) Ten (10) Vocoder Channels for SIP Trunks</p> <p>c) 25 licenses subscription</p> <p>d) 24 Enterprise IP Phones</p> <p>e) 1 Operator IP Phone with Console</p> <p>f) Voice Menu System (VMS) attendant for an automated virtual system.</p>			P 1.5 Million

Handwritten marks: a signature and the letters 'mf'

	<ul style="list-style-type: none"> g) Feature for call detail records h) Two (2) units 24 Port Power Over Ethernet (POE) Switch for IP-phones i) Fiber one Local Exchange Carrier (LEC) 10 Mb for remote extension within the building or complex j) 1 x Fiber 1 LEC 10 MBPS - for remote extension within the building (comes with wifi Router (4 Port), /29 IP k) Block, 1GB MRTG Access and Monitoring) 			
<p># 3</p>	<p>Network Equipment and Access Points</p> <ul style="list-style-type: none"> a) One (1) unit Core Switch b) Two (2) units 24 port GE ports Power over ethernet (POE) Switch c) Four (4) units 48 ports GE Distribution Switch d) Ten (10) units of Cisco Meraki Access Points with one (1) year subscription Manage Remote License e) Twelve (12) 10 G Transceiver Modules f) One (1) Enterprise Network and Server Monitoring System includes one (1) year support and maintenance plan for 100 Node licenses. g) Two (2) units of 2KVA rackmount UPS 			<p>P 8.8 Million</p>

Handwritten marks: A blue checkmark and a blue scribble.

	h) Implementation Activities - Configuration, testing, and commissioning all active components, including hardware and software. i) Training and knowledge transfer j) Project documentation, turn-over, and acceptance. k) Warranty and Support			
# 4	Structured Cabling - Supply, delivery, and installation of network peripherals and cabling materials for 100 nodes			P .5 Million
Total				P 15.8 Million

APPROVED BUDGET

The financial proposal shall not exceed the approved budget for the Contract (ABC) of Fifteen Million Eight Hundred Thousand Pesos (**P 15,800,000.00**) inclusive of taxes and duties.

- I. **SCOPE OF WORK** – The **Winning Bidder** shall provide the service to the Philippine Tax Academy (PTA) in accordance with the terms and conditions and must include the following provision of service:
1. Must provide Design and Planning of the service to be provided.
 2. The Winning Bidder must Supply, Deliver, Configure, and Install:
 - 2.1. **Two (2) Independent Internet Service Providers (ISPs) with One Hundred Fifty (150) Mbps Committed Information Rate (CIR) each** via Fiber Optic Cable to the PTA Office located at 3rd floor, DOF Main Building and 7th floor, EDPC Building, BSP Complex Roxas Blvd., cor. P. Ocampo St., Manila.
 - 2.2. **Two (2) units Managed Service Telco Grade Router for each independent ISP:** Cisco ISR 4351 routers including subscriptions and Local supports.
 - 2.3. **One (1) unit Managed Service Load Balancer Internet Access Gateway appliance.**
 - 2.4. **Managed service PABX System**
 - 2.5. **One Hundred (100) nodes of structured cabling**
 3. **Installation cost** must be bundled with the one-year contract service, including providing the needed cables/insulation and other related materials following industry standards.

h *rb*

4. Suppose the PTA transfers to a new office location. In that case, the Provider must **transfer the Fiber Optic Cable (FOC) connection**, including hardware re-deployment, to the new site at no cost.
5. Must conduct **Acceptance testing**, which will be used as the basis for the start of the billing period for the internet service (ISP); shall take place after the installation and inspection, subject to the following criteria:
 - 5.1. Must be conducted by the winning Internet Service Provider /Telecommunications Company (ISP/Telco) in the presence of PTA-ITD representatives;
 - 5.2. No service interruption must take place during the testing period, except for those beyond the provider's control (i.e., power failure, failure of equipment, and international/regional backbone problems);
 - 5.3. Committed Information Rate (CIR) requirement compliance for two (2) proposed independent ISPs;
 - 5.4. Latency requirement compliance;
 - 5.5. Must turn over an assigned Multi-Router Traffic Grapher (MRTG) accounts for both independent ISPs to PTA-ITD;
 - 5.6. Must secure and provide usable static public IP-Address as required.
 - 5.7. Must conduct Bit Error Rate (BER) Test.
 - 5.8. The Acceptance Test Procedure must have the following results:
 - 5.8.1. Line Quality Test - Test: BER - Standard: **Error – free**
 - 5.8.2. Test for Packet Loss - Test: Ping - Standard: **100% packet return**
 - 5.8.3. Latency Test - Ping - Standard: **180-250 milliseconds to US routes.**
6. **Technical Support:** Technical support services must include the following:
 - 6.1. **Maintenance Services**
 - 6.1.1. Maintenance of all provided hardware, peripherals, and Software to ensure proper working order;
 - 6.1.2. Replacement of all defective hardware peripherals and materials in case of hardware malfunction;
 - 6.1.3. Pro-active notification thru email, phone calls, and SMS on any occurrences of the following:
 - a. Schedule downtime
 - b. Service interruption
 - c. Upgrades or preventive maintenance
 - d. Possible rerouting of internet connection to backup link due to connection loss of both primary and secondary links.
 - 6.2. **Customer support**
 - 6.2.1. 24x7 on-call support;
 - 6.2.2. Must resolve all kinds of technical problems within 30 minutes from the initial report time, including but not limited to:
 - a. When the links connection is down
 - b. Packet loss
 - c. Latency variation
 - d. Routing issue
 - 6.2.3. Must provide an hourly status update from receipt of initial report time if trouble will take more than 30 minutes to resolve;
 - 6.2.4. Must provide telephone (landline/cellphone), SMS, or Email technical support, available on a 24x7 basis to assist in troubleshooting issues;

6.2.5. Must provide qualified technical representative/s, within 24 hours of initial report time and at no additional cost to PTA, for issues that need to be resolved on-site.

6.3. Service Level Agreement

6.3.1. Must provide Network Availability of: 99.8%

6.3.2. Must have 24/7 network support and data operations center

6.3.3. Must have an Upgradeable and Scalable Bandwidth Provisioning

6.3.4. Must have a robust and resilient network

6.3.5. Must have an extensive nationwide network

6.3.6. Must have experienced and licensed technical support engineers for the required managed routers and equipment, preferably Cisco Certified Network Associate (CCNA) and Cisco Certified Network Professional (CCNP)

6.3.7. Must provide guaranteed latency not less than 200ms at 50% load from PTA to the internet service provider

6.3.8. Must have a guaranteed Packet Loss of 0.1% or less

6.3.9. Provide PTA a written notice at least (5) working days before the scheduled maintenance work. In the event of service interruption due to scheduled maintenance, the provider should have alternate re-routing of the internet connection.

6.3.10. Mean-Time-To-Repair (MTTR)

6.3.11. Router Connection Error (30-45 mins)

6.3.12. Local Exchange Breakdown (2-4 hrs)

6.3.13. Scheduled Maintenance Work (4-6 hrs)

6.3.14. Must provide a monthly report of service interruption and time of delay with corresponding rebates, if there are any.

6.3.15. Diverse and distributed cable routes using trans-Asia and trans-Pacific submarine cable systems with redundancy

6.3.16. Must provide a direct connection to major IXs (Internet Exchanges), both local and international

6.3.17. Minimum of 1:1 Committed Information Rate (CIR) synchronous download and upload.

6.3.18. Must provide real-time access to bandwidth utilization monitoring reports through Multi Router Traffic Grapher (MRTG) for two (2) circuits.

II. DELIVERY AND RECEIVING INSTRUCTIONS

The Supplier shall observe the following instructions:

1. Services/Goods as specified in this Schedule of Requirements and/or the Technical Specifications must be delivered only to the address indicated herein.
2. The Provider must notify the indicated authorized receiving personnel at the Project Site of the **scheduled delivery date at least three (3) working days in advance** and shall ensure that the authorized receiving personnel from the PTA is present during the date and time of delivery.
3. The Supplier shall **deliver to the Project Site from 9:00 AM to 6:00 PM and on Mondays to Fridays only**; the Provider shall not make deliveries before 9:00 AM, after 6:00 PM, and on non-working days.

4. Upon delivery of the Goods to the Project Site, the supplier shall notify the PTA and present the following documents:
 - 4.1. Original Supplier's Invoice showing the Goods description, quantity, unit price, and total price.
 - 4.2. Original Delivery Receipts
 - 4.3. Original Statement of Accounts.
 - 4.4. Approved Purchase Order for these conditions, Purchaser's representative at the Project Site is **Mr. Mark P. Olaguir**, Development Management Officer III, and concurrent **Technical Property Inspector** or his authorized representative(s).

III. TECHNICAL SPECIFICATIONS

Description
<p>1. Internet Dedicated Service with High-Availability (IDS-HA)</p> <p>1.1 Two (2) Independent ISP (Primary and Secondary): 150 Mbps each IDS Connection speed with modem/media converter</p> <ol style="list-style-type: none"> 1.1.1. Must be a Tier-1 internet provider with multiple submarine cable link support and has fully redundant network routers connected to a high-performance fiber optic infrastructure. <i>"Tier-1 means registered "Telecommunications" Company in the Philippines"</i> The Provider must have a total network traffic capacity of at least 80 Gbps IP upstream (US and Asia) 1.1.2. The Provider must be ISO 9001:2015 certified, and ISO 27001: 2013 certified. 1.1.3. The provider must have at least ten (10) years as a telephone and internet service provider from the NTC. 1.1.4. Must have Seamless Dedicated Internet Premium Bandwidth with High Availability (HA) via fiber connection capable of transmitting multiple traffic streams and variable bandwidth preset with twice the subscribed bandwidth of: Independent Primary ISP = 150 Mbps and Independent Secondary ISP = 150 Mbps. 1.1.5. Must have an existing Wide Area Network (WAN) fiber-optic backbone near the main entrance of Bangko Sentral ng Pilipinas (BSP) and Department of Finance (DOF) Buildings. 1.1.6. Must have a Metro-wide fiber optic network 1.1.7. Must have a Tier 1 International Internet Exchange backbone connection with the corresponding type of connections (submarine cable, satellite, etc.) 1.1.8. Must be able to change traffic with other Tier 1 providers, following strict peering agreements. (Peering is the internet traffic exchange between two networks that have agreed on a connection to exchange traffic without using a third party, reducing internet costs. Without Tier 1 internet providers, internet traffic could not be exchanged between countries.) 1.1.9. Must be capable of connecting to wan failover and ISP internet load balancing appliance with stable bandwidth connection.



- 1.1.10. Must be directly connected from the main pipe of the USA internet backbone and directly connected to the foundations of the internet, offering higher speed connections and more reliable networks.
 - 1.1.11. Must be connected from the Asia Pacific loop of a backbone with the East-Asia Crossing and Pacific Crossing.
 - 1.1.12. Must be a member of a Local Internet Exchange, e.g., Philippine Internet Exchange (PhiX), Matrix Internet Exchange (MIX), Common Routing Exchange (CORE), etc.
 - 1.1.13. Must guarantee a 1:1 ratio of bandwidth from the user's office to the global Internet
 - 1.1.14. Must have a flatter network optimized for IP with low latency
 - 1.1.15. Must be capable of a redundant node from PTA Site to the ISP's main hub.
 - 1.1.16. Must perform a Bit Error Ratio (BER) Testing after installation.
 - 1.1.17. Must Supply a Committed Information Rate (CIR): No less than 150Mbps each independent ISPs.
 - 1.1.18. Must provide Public IP addresses (PIP): IP allocation should be flexible and easier to access from a Tier 1 provider.
 - a. /30 and /27 for the ISP1, and
 - b. /30 and /27 for the ISP2
 - 1.1.19. The facility Must be owned and operated by the Internet Service Providers (ISPs).
 - 1.1.20. Must perform Local Area Network (LAN) and Wide Area Network (WAN) equipment configurations.
- 1.2. **Two (2) units Managed Service Telco Grade Router for each independent ISP:** Cisco ISR 4351 routers including subscriptions and Local supports with the following specifications:
- 1.2.1. Form Factor: 1ru
 - 1.2.2. Performance: 500 Mbps throughput upgradable to 2Gbps
 - 1.2.3. Management Port with Management Cable
 - 1.2.4. Network Interface Module (NIM): 3
 - 1.2.5. Default / Max Dram: 8 GB / 16 GB
 - 1.2.6. Integrated Services Card Slots: 1 (PVDM 4)
 - 1.2.7. USB ports (type A): 2
 - 1.2.8. Power Supply Type: Internal AC, POE, or DC
 - 1.2.9. Redundant Power Supply:
 - 1.2.10. Module online insertion and removal
 - 1.2.11. Server virtualization platform (UCS E Series) and Network Compute Engine (NCE): 4 Core NCE
 - 1.2.12. Zone-based firewall and NAT services:
 - 1.2.13. VRF- aware Firewall and Network address translation (NAT)
 - 1.2.14. Hardware VPN acceleration (DES, 3DES, AES)
 - 1.2.15. IPSEC VPN Services:
 - 1.2.16. Flex VPN, Easy VPN remote server, Enhanced Easy VPN, Dynamic Multipoint VPN (DMVPN)
 - 1.2.17. Group encrypted transport VPN (GET VPN), V3PN, MPLS VPN
 - 1.2.18. Intrusion Prevention: Snort for signature Based and Firepower as nGIPS
 - 1.2.19. Anomaly Detection and Machine Learning: Cisco Self Learning Networks (SLN)

- 1.2.20. Network Foundation Protection: ACL, FPM, control plane protection, control plane policing (capp), Qos role-based CLI access, source based RTBH, uRPF, SSH v2
- 1.2.21. Cisco Umbrella Branch Support
- 1.2.22. Cisco Cloud web security
 - a. Cisco trust Sec
 - b. Security Group tag Exchange Protocol (SXP), SGT over GETVPN
- 1.2.23. SGT over IPSEC
- 1.2.24. SGT over DMVPN
- 1.2.25. SGT-based ZBFW
- 1.2.26. Port/Layer 3 interface/IP/Subnet-to-SGT mapping
- 1.2.27. SGT export in Flexible Netflow

1.3. One (1) unit Load Balancer Internet Access Gateway appliance.

1.3.1. Hardware & Performance Profile:

- a. The proposed solution must be a 1RU appliance
- b. The proposed solution must meet the performance specification below:
- c. Firewall throughput 12Gbps.
- d. New connections(TCP)80,000.
- e. Threat prevention throughput 4.2Gbps
- f. IPS Throughput 3.85 Gbps
- g. The proposed solution must provide the type & number of interfaces as below:
 - At least two (2) USB ports
 - At least six (6)10/100/1000 Base-T ports
 - At least 2 SFP ports
 - At least two (2) 10G ports with end to end SFP Modules.
- h. Hard Disk - The proposed solution must provide 64Gb SSD disks

1.3.2. Network Adaptability

- a. Deployment
- b. The product proposed should support following deployment modes:
 - routing/gateway mode;
 - transparent/bridge mode
 - virtual wire mode
 - bypass mode.
 - Mixed mode

1.3.3. Hardware Bypass

The product proposed must support at least 2 pair of hardware bypass(copper), so in case of device failure, the network traffic can still pass.

1.3.4. High Availability

The proposed product must support high availability via.

- Active-Active mode;
- Active-Passive or Active Standby mode;

1.3.5. Link Aggregation

The proposed product must support link aggregation with following work mode:

- Load balancing - hash
- Load balancing - RR(Round Robin)
- Active-Passive
- LACP

1.3.6.Link State Propagation

The proposed product must support link state propagation, that means can setup the correlation interface group, if one of the interface in the group turns up/down, the other interface will follow the same action

1.3.7.Link State Detection

The proposed product must support link state detection, with at least the methods below:

- Address Resolution Protocol (ARP)
- Packet Internet or Inter-Network Groper (Ping) or ICMP
- Domain Name Server (DNS) Lookup

1.3.8.Network Address Translation (NAT)

The product proposed must support different mode of NAT:

- SNAT, DNAT and bidirectional NAT.
- One to one NAT, one to many, many to one NAT.
- NAT46, NAT64

1.3.9.IPv6

The product should be ready for IPv6, include:

- Support IPv4/IPv6 dual stack mode;
- Support control IPv6 in access control policy, provide control via IP address, service, application, domain,etc.

1.3.10. Dynamic Host Configuration Protocol (DHCP)

The product should support DHCP, include:

- Act as DHCP server or DHCP proxy
- Support IP reservation

1.3.11. Generic Routing Encapsulation (GRE)

The product proposed should support GRE tunnel.

1.3.12. Others

- Support DNS transparent proxy
- Support ARP proxy
- Support DDNS

1.3.13. Routing

Static Route

- The product proposed must support static routing.

1.3.14. Dynamic Routing

The product proposed must support dynamic routing protocol:

- Routing Information Protocol (RIP)v1/2
- Open Shortest Path First (OSPF)v2, OSPFv3
- Boarder Gateway Protocol (BGP)4

1.3.15. Open Shortest Path First (OSPF)

Support redistributes direct route, static route, RIP route (OSPFv2), default route to OSPF.

h 26

- Support authentication method: plaintext, MD5
- 1.3.16. Border Gateway Protocol (BGP)
Support redistribute direct route, static route, RIP route, OSPF route to BGP
- 1.3.17. Policy-Based Route
The product proposed must support policy-based route. The policy route can setup with:
- Routing source can be specific to IP, IP group
 - Support select route based on IP, services, Country/Region, Application etc.
 - Support load balance via at least 4 methods, Round Robin, Bandwidth ratio Round robin, Weighted least traffic, prefer the first link (link on top)
- 1.3.18. IPsec Virtual Private Network (VPN)
The proposed product must support at two types of IPsec VPN protocols:
- Proprietary VPN protocol.
 - Standard IPsec protocol.
- 1.3.19. Dynamic Connection
The product proposed must be able to setup site to site VPN in the following scenarios:
- Both site is static IP
 - Both site is dynamic IP
 - One site is dynamic IP while the other site is static IP
- 1.3.20. VPN Status Monitoring
Support monitoring the status of each VPN tunnel, the data be monitoring includes:
- Overview of all the active VPN tunnels
 - Inbound/outbound traffic;
 - Latency
 - Packet loss rate;
- 1.3.21. Software Defined-Wide Area Network (SD-WAN)
The solution proposed should support SD-WAN capability via VPN tunnels:
- Support session-based link balancing mode.
 - Can choose the optimize link based on bandwidth-remaining ratio, application type or link quality (means packet loss, jitter, latency)
- 1.3.22. Others
- a. Support IPsec VPN as the backup link, when main link (MPLS or lease line) disconnected, the traffic will failover to IPsec tunnel
 - b. Support Access Control, Security policy (IPS, APT etc) on IPsec tunnel.
- 1.3.23. Secure Socket Layer (SSL) VPN
The proposed product should support SSL VPN feature.
- Support at least 30 concurrent user access
 - Support TCP, UDP, ICMP protocols
 - Support HTTP, HTTPS, Email, Fileshare, FTP etc.

Handwritten marks: a blue checkmark and a blue scribble.

- Support control access by IP, URL, TCP/UDP port etc.
 - Support access resource (destination IP/system) by NAT (NGAF IP address) or virtual IP
- 1.3.24. Operating System and Browser
The proposed product should be able to support SSL VPN access via Windows XP/7/8/10, MacOS, Andriod, IOS
- 1.3.25. Active Directory Support
- Support LDAP user automatic synchronization.
 - Support Microsoft AD security group mapping.
 - Support SSL VPN user log in & log out log
- 1.3.26. User Authentication
The proposed product should be able to support user authentication via following standard:
- Support captive-portal based authentication; the captive portal is customizable;
 - Support Single Sign-on (SSO) with Microsoft AD, Radius
 - Support local user database, and external user authentication such as LDAP, Radius, POP3 etc.
- 1.3.27. Access Control
The proposed solution should support application control feature and meet the following specifications:
- Support application control and can identify & control over 9800+ applications.
 - Support admin customize their own application types
 - Typical types of applications can be controlled include game, P2P, shopping, social networking etc.
 - Should be able to control applications via source/destination IP, username, Schedule etc.
 - Be able to deny, allow applications
- 1.3.28. Uniform Resource Locator (URL) Filtering
The proposed product must support URL filtering:
- provide at least 70+ URL categories, include game, gambling, finance, Pornography etc.
 - Support manually create customized the URL category.
 - Should provide on premise URL signature database, not only rely on cloud.
- 1.3.29. File Filtering
The proposed solution must support filter, which can filter the download, upload file by file type(extension).
- Support common file type(extension) category, such as, image, text, executable file, scripts etc.
 - Support customized file type(extension)
- 1.3.30. Connection Control
The proposed solution should support feature to control concurrent session/connections:
- Be able to control concurrent session/connect by source IP, destination IP, or both
 - In the policy, it will be able to setup specific concurrent session/connection number.

1.3.31. Geolocation Control

The proposed product should be able to control traffic based on Geolocations:

- Be able to control the source IP by a geolocation level, that means the device have a database that can identify the access (IP) is from which country/region and specify the deny or allow action
- The geolocation identifications should be able to support to the major countries in the world
- Support the search feature to help find out a specific IP belong to which region.
- Support check the status of IP that being blocked.
- Support exclude specific IP from the control.

1.3.32. Bandwidth Management

The product proposed must be able to support bandwidth management feature:

- Be able to limit or guarantee the bandwidth based on IP, user, application, schedule, VLAN etc.
- Be able to provide per IP/User speed control in single policy

1.3.33. Security Protection

Overall Intrusion Prevention System (IPS)

The product propose must support IPS feature and meet the specification below:

- IPS signature over 9000 entries on premise.
- Support admin create customized IPS signature by regular expression, keywords, protocol, port & direction
- Support admin change the signature default action by per signature based or global.
- User can use CVEID, Vulnerability Name, vulnerability ID, threat level etc to search for the related signature.
- IPS module should be able to detect brute-force attack to DB2, Mongoddb, MSSQL, MySQL, FTP, IMAP, Jboss, Jenkins, Joomla, Kerberos, SMB, Telnet, SSH, RDP etc.
- IPS can get up to date signature data via cloud threat intelligence or upload signature package via web UI
- Support minimize to 10-minute update after a new outbreak happens, when connect to cloud threat intelligence

1.3.34. Advance Persistent Threat (APT) Support Feature

The proposed solution must support APT and meet the following:

- Detection of remote control trojan, malicious URL/domain, and other threats.
- The product should support at least 140 million malware signature database on premise
- The device can connect to cloud threat intelligence and do real-time for check to threat that cannot be identified locally.
- APT can effectively identify & block the abnormal traffic within well-known protocols such RDP, SSL, IMAP, SMTP, POP3, FTP, DNS, HTTP, WEB

1.3.35. Anti-Virus Support Feature

Handwritten initials and marks at the bottom right of the page.

The proposed solution must support anti-virus feature:

- Support stream based anti-virus with AI-Based anti-virus engine
- Support protocols HTTP, HTTPS, FTP, SMTP, IMAP, POP3, SMB etc.
- Support compress file detection, and support compress file with up to 16 layers.
- Support scan the files up to 20MB
- Support detect virus in main stream file types, include text, image, music, movie, compressed file, executable file, document, script,etc.
- Support cloud based analysis with the file cannot be identified locally
- Support whitelist or exclude trusted file by MD5 or URL path

1.3.36. Anti-DoS/DDoS (Denial of Service)

The proposed solution must support anti-dos/ddos features, with the features:

- Support ARP flood, SYN flood, UDP flood, DNS flood, ICMP&ICMPv6 flood protection.
- Support IP/port scan protection.
- Support detection and prevent Tear Drop attack, LAND attack, Win Nuke attack, Smurf attack, Ping of death, IP fragment.

1.3.37. Cloud Threat Intelligence

The proposed solution should provide the cloud-base threat intelligence capabilities, include:

- Cloud Sandboxing
- Cloud intelligence to identify unknown/new threats
- Cloud intelligence can provide the new signature update to new outbreaks, the minimized respond time is 10 minutes.

1.3.38. Decryption

The proposed solution must support HTTPS decryption

1.3.39. Account Protection

The proposed solution must support a dedicated account protection module to identify the abnormal usage of user accounts.

- Support detection of weak password, brute-force attack, abnormal/suspicious login etc.
- Provide dedicated GUI page to show & respond all the account abnormal usage events that happens recently.

1.3.40. Ransomware Protection

The proposed solution must support a dedicated ransomware protection module, which can:

- Automatically scan and detect ransomware related vulnerabilities, port, weak password, brute-force attack etc.
- Provide dedicated GUI page to show and respond all the ransomware related vulnerabilities
- Can provide guidance or suggested action to admin, e.g., deploy block policy direct,

1.3.41. Security Assessment

Risk Analytics

- a. The proposed solution must provide risk analytics module that allows to scan and identify security loopholes such as open port, system vulnerabilities, weak passwords, etc.
- b. The risk assessment should support major protocols such as: HTTP, HTTPS, POP3, SMTP, RDP, SMB, Oracle, MS-SQL, MySQL etc.

1.3.42. Passive Vulnerability Scan

- a. The proposed solution must provide a real-time vulnerability analysis or passive vulnerability scan:
 - Detection vulnerabilities based on traffic pass through NGAF, without any active scanning activities to the servers, minimize the extra work load and other impact
 - The vulnerabilities that can be detected includes web application vulnerability, weak password, improper configuration on web server, etc.
 - Support generate HTML format report

1.3.43. Log and Reporting

- a. The proposed solution must support build-in log center which can keeps 4 types logs:
 - Access Log (Application control log, user authentication log, SSL VPN log)
 - Security Log (IPS, WAF, Botnet, Email protection, Anti DoS, Web Access)
 - System log
 - Support export log to excel file.
- b. The appliance should include the local hard disk to provide log retention

1.3.44. Reporting

The proposed solution must support build-in reporting features, which include:

- Generate comprehensive Security report in PDF format
- Support security report subscription by email, in daily, weekly, monthly based.

1.3.45. Syslog

The proposed solution must support export log to syslog server

1.3.46. Certifications - CyberRatings

The proposed solution must be with "AAA" racking in the Cyber Ratings Enterprise Firewall

1.3.47. Capability Maturity Model Integration (CMMI)

Vendor must be certified with CMMI L5.

2. MANAGED SERVICE - PABX SYSTEM

2.1. PABX System must have minimum capacity of the following configuration:

2.1.1. One (1) ISDN Port Thirty (30) Channels

2.1.2. Ten (10) Vocoder Channels for SIP Trunks

2.1.3. 10 SIP Ports

2.1.4. 25 IP Subscriber Licenses

2.1.5. One (1) Operator IP Phone

Handwritten initials and marks at the bottom right of the page.

2.1.6. Twenty-Four (24) Enterprise IP Phones

- 2.2. Operator IP phone must be paired with DSS expansion key
- 2.3. The IP-PBX/PABX/Communication System shall employ IP at its core with IP switching technology and 100% non-blocking.
- 2.4. The system should be IPV6 ready.
- 2.5. The architecture of the system shall be capable of seamless migration to its maximum capacity by simply adding peripherals cards/modules in the same chassis without compromising function/features of the system. The architecture should be non-stackable eliminating individual power supply for each chassis.
- 2.6. The system should be built on a universal slot architecture and modular in design to enable seamless growth, by adding the desired necessary modules and cards as and when required. Any interface peripheral card can be inserted in any slot of the platform, whereby it is possible to increase or decrease the trunk lines or subscriber lines of the system as per the requirement.
- 2.7. It shall have distributed processing architecture, SLIC and SMT Design.
- 2.8. The system shall have the built-in Auto-attendant facility and shall be able to answer minimum 9 calls simultaneously and should support dial-by-name.
- 2.9. The system shall be compatible and type-approved with ISDN PRI line of Local Service Provider.
- 2.10. The PRI card should be software programmable for TE/NT mode.
- 2.11. Two (2) units 24 ports Power Over Ethernet (POE) Switch must be included to provide power to the IP phones
- 2.12. The system shall have built-in web-based software programming tool for system administration.
- 2.13. Detail reports of all system parameters should be generated through the SMDR port of system.
- 2.14. Each port of the system shall be programmable. It shall have programmable features port-wise/extension-wise.
- 2.15. The system shall support flexible numbering for extensions such as it may have extensions with 1 digit, 2 digits and up to 6 digits' numbers as well as in combination of all.
- 2.16. Access codes, system timers and access to features shall be programmable.
- 2.17. Storage of outgoing, incoming and internal call reports shall be generated on SMDR port of the system. It shall also be available online through Ethernet Port.
- 2.18. System must have a built-in station message detail recording to log calls without any added modules
- 2.19. Provision of PABX telephone system must include the installation, configuration and after-sales service support
- 2.20. Full Comprehensive Warranty (12 Months) for PABX system and telephone handsets
- 2.21. Knowledge Transfer and End-User Training must be provided after commissioning
- 2.22. 1x Fiber 1 LEC 10MB - for remote extension within the building up (comes with Wi-Fi Router (4 Port), /29 IP Block, 1GB of either email or web Hosting Service and MRTG Access)

3. NETWORK EQUIPMENT

3.1. Core Switch

- 3.1.1. Managed switch with 12 x 10G copper ports + 12 x 10G SFP+ modules (dedicated)
- 3.1.2. 1 Gigabit Ethernet Management port
- 3.1.3. 1RU Height Rackmount
- 3.1.4. 480Gbps switching capacity
- 3.1.5. With MTBF of around 1.372M (hours) at 25°C
- 3.1.6. 3MB Packet Buffer
- 3.1.7. 240mpps (64-byte packets)
- 3.2. 24-Port PoE Gigabit Switch
 - 3.2.1. Equipped with 24 Gigabit Ethernet Ports Full PoE+ x 4 10 Gigabit Ethernet
 - 3.2.2. Supports PoE budget of 370W on full load on a single power supply
 - 3.2.3. Max power consumption < 440W on full load
 - 3.2.4. Supports up to 128 Gbps switching capacity
 - 3.2.5. With MTBF of around 698K (hours)
 - 3.2.6. Rack mountable
- 3.3. 48-Port Gigabit Switch
 - 3.3.1. Equipped with 48 Gigabit Ethernet + 4 10 Gigabit Ethernet ports
 - 3.3.2. Supports 176 Gbps switching capacity
 - 3.3.3. Supports up to 8K MAC addresses
 - 3.3.4. With MTB of around 1.452M (hours)
 - 3.3.5. Rack mountable
- 3.4. Indoor Wi-Fi 6 Access Points
 - 3.4.1. Cloud managed Access Point with integrated enterprise security and guest access
 - 3.4.2. 2x2:2 (2.4GHz) + 4x4:4 (5GHz) MU-MIMO 802.11ax
 - 3.4.3. Application-aware traffic shaping
 - 3.4.4. Enhanced transmit power and receive sensitivity
 - 3.4.5. Supports automatic cloud-based RF optimization
 - 3.4.6. With MTB of around 500K (hours)
- 3.5. Network Monitoring Software
 - 3.5.1. Supports 4 monitoring engine to provide users with efficient, scalable monitoring
 - 3.5.2. With dashboard that provides a customizable high-level overview of hosts, services, and network devices
 - 3.5.3. Can easily view network incidents and resolve them before they become major catastrophes
 - 3.5.4. Automated, integrated trending and capacity planning graphs allow organizations to plan for upgrades
 - 3.5.5. Equipped with configuration wizards & infrastructure management
 - 3.5.6. Supports advanced user management to easily setup and manage user accounts with only a few clicks then assign custom roles to ensure a secure environment

4. STRUCTURED CABLING

Supply, delivery and installation of network peripherals and cabling materials for 100 nodes

- 4.1. Cat6 UTP Cable
 - 4.1.1. 10/100/1000 BASE-TX
 - 4.1.2. Bare Copper Material, 23 AWG Construction Conductor

- 4.1.3. HDPE Material Insulation
- 4.1.4. PE Cross Member
- 4.1.5. ISO/IEC 11801 ED.2.2:2011 Compliant
- 4.1.6. ANSI/TIA 568-c.2-2011 Compliant
- 4.2. Cat6 Patch Panel
 - 4.2.1. IDC connector can accept 22-26 AWG solid and stranded cables.
 - 4.2.2. Terminate using 110 or Krone Tools
 - 4.2.3. Dimensions and mounting compliant with EIA-310-D
 - 4.2.4. Panel Area: SECC/1.5mm thickness
 - 4.2.5. Number of ports/ height: 24/1U
 - 4.2.6. Color: Black
 - 4.2.7. Easy port description by removable labels in plastic holders.
 - 4.2.8. RoHS Compliant
- 4.3. CAT6 Modular Plug / RJ45 Connector - Unshielded
 - 4.3.1. UL Applications that support up to 250V AC
 - 4.3.2. Dielectric with standing voltage 500V AC
 - 4.3.3. 100Mohms Insulation Resistance
 - 4.3.4. Transparent Polycarbonate
 - 4.3.5. Phosphor bronze blade w/ gold plating
- 4.4. UTP Cable Management Guide 1U
 - 4.4.1. 19" Standard rack and cabinet mountable
 - 4.4.2. Meets EIA/TIA bend radius requirements.
 - 4.4.3. Prevents cable tangles
 - 4.4.4. Light weight and easy to install.
 - 4.4.5. The panel is configured with 12 rings.
 - 4.4.6. Two (2) openings in the rear to provide access pathway
 - 4.4.7. ROHS Compliant
- 4.5. Cat6 UTP Patch Cord
 - 4.5.1. Category 6 UTP patch cord using RJ45 contacts 50u inch gold plated and snag proof boot.
 - 4.5.2. 10/100/1000 BASE-T, Voice, Video and other applications

Conductor	Material / Size	Bare Copper / 30 AWG
Insulation	Material	High Density Poly Ethylene (HDPE)
	Diameter	0.55 ± 0.05 mm
Sheath	Material	Low Smoke Zero Halogen (LSOH)
	Diameter	3.1 ± 0.2 mm
- 4.6. 19" Open Bay Rack, Floor Mount
- 4.7. One (1) unit UPS Rack mountable/tower, 2000VA 230V- 1800 Watts or higher

IV. BILL OF MATERIALS, CONFIGURATIONS AND SITE WORKS

DESCRIPTION	QTY
INTERNET DEDICATED SERVICE WITH HIGH-AVAILABILITY (HA)	
Independent ISP with modem / media converters	2

ju *mb*

DESCRIPTION	QTY
Managed Telco Grade Router	2
Bandwidth Manager Internet Access Gateway	1
PABX System	
MANAGED PABX SYSTEM - 10SIP x 25 IP PHONES	
10 Vocoder Channels for SIP Trunks	
25 IP Subscriber Licenses	
1 Operator IP Phone w/ DSS Console	
24 Business IP Phones	
VMS for Automated Attendant	
SMDR Feature for Call Detail Records	1
2 x 24-Port PoE Switch for IP Phones	
Installation, Testing, Commissioning and Acceptance	
Comprehensive Warranty & Support	
Project Acceptance and Turn-over	
1x Fiber 1 LEC 10MB - for remote extension within the building up (comes with wifi Router (4 Port), /29 IP Block, 1GB of either email or web Hosting Service and MRTG Access)	
NETWORK	
Supply of Equipment and Peripherals	
Core Switch	1
24-Port Gigabit PoE Switch	2
48-Port Gigabit Switch	4
Cisco Meraki MR44 w/ MR Enterprise License, 1YR	10
10G Transceiver Module	12
Nagios XI Enterprise 100 Node License, 1 Year Ticket Support and Maintenance Plan	1
2KVA UPS, Rackmount	2
Site Supervision, Engineering and Project Management	
Preliminary Activities	
Supply of Labor and Manpower	
General Provision, Mobilization and Demobilization	
Physical Installation of Active Equipment	
Active Components System Configuration, Testing, and Commissioning	
Network Monitoring Software Installation & Commissioning	
Functionality Testing & UAT	1
Configuration Validation / Host	
Provisioning of Temporary Tools and Equipment during installation	
End-user Training & Knowledge Transfer	
Project Documentation	
Project Turn-over	
Project Acceptance	
1- Year Maintenance Agreement	
1 -Year Standard Warranty	
STRUCTURED CABLING	
Supply of Network Peripherals and Cabling Components	
CAT6 UTP 4 PAIR SOLID 305M	3

DESCRIPTION	QTY
CAT6 24 Port UTP Patch Panel 1U	1
Cable Boot (Black, Blue, Green, Gray, White, Yellow, Red)	20
CAT6 Modular Plug / RJ45 Connector - Unshielded	20
UTP Cable Management Guide 1U (Plastic)	10
CAT6 UTP Patch Cord, 5M	100
CAT6 UTP Patch Cord, 2M	100
CAT6 UTP Patch Cord, 1M	20
19" Open Bay Rack, 7 ft. w/ vertical cable manager	1
Supply of Roughing-ins	
Roughing-in Materials, Fittings & Supports (Conduits, Mouldings, etc.)	1
Consumables and Miscellaneous	
Site Supervision, Engineering and Project Management	
Preliminary Activities	
Supply of Labor and Manpower	
Mobilization and Demobilization	
Layout and Installation of Roughing-Ins	
UTP Cable Layout and Installation	
Port Testing, Re-tagging and Labelling (100 Ports)	
Termination of UTP Cables	1
Re-patching of Existing Cabling	
Provisioning of Temporary Tools and Equipment during installation	
Project Documentation	
Project Turn-over	
Project Acceptance	
6-Months Workmanship Warranty on Cabling Works	
LOAD BALANCER	
Hardware appliance, 6 x GE RJ45 + 2 x SFP, 1 x available NIC slot. Default with 64GB SSD. Support 12Gbps Firewall Throughput, 4.2Gbps Threat Prevention Throughput.	1
System License Package for the following features: Firewall, Bandwidth Management, URL Filtering, Application Control	1
System On-site Configuration of Supplied Equipment	
Testing & Commissioning	1
System Training	
1-Year Equipment Warranty and Technical Support	

In the event that any of the materials run out, it shall be the responsibility of the winning bidder to replenish the same, notwithstanding from the quantity of the bill of materials.

V. TRAINING REQUIREMENTS

Prior to Final Acceptance, the supplier shall provide End-user training on how to use and manage the active components included in the project.

Handwritten initials/signature

The winning bidder shall also provide the end-user with user, configuration and technical manuals.

VI. WARRANTY AND MAINTENANCE:

1. Six (6) months workmanship warranty for structured cabling
2. One (1) year warranty for ICT equipment such as APs, routers, switches, and racks.
3. With parts and on-site service support for all equipment during the whole duration of the warranty.
4. After-sales support services with committed Service Level Agreement of **99.8%**. Customer Service Center facilitates communication between customers and various technical levels within **24 hours x 7 days a week basis**.

VII. DOCUMENTARY REQUIREMENTS:

1. **Duly Notarized Declaration of the following;**
 - 1.1. Must have Fiber Optic Cable Multiplexer and Gigabit Ethernet (GE) capable. Interface Hand-off: (Gigabit Ethernet 10/100/1000 - electrical)
 - 1.2. Must have at Least 1Gbps Multi-Lateral Peering with Phopenix for at least six (6) years.
 - 1.3. Must have at least ten direct International Uplinks (Tier 1/Tier 2, ie. AT&T, Level 3, Telstra, etc.) for redundancy purposes.
 - 1.4. Minimum total Uplink capacity of 40Gbps to 130Gbps
 - 1.5. Managed and operated local Internet peering (i.e., MIX, GIX, PHIX)
 - 1.6. High Speed and Dedicated Internet service with 1:1 CIR (Committed Information Rate)
2. **Must Provide a Detailed Diagram of the Following:**
 - 2.1. at least 10 direct International Uplinks (Tier 1/Tier 2, ie. AT&T, Level 3, Telstra etc.) for redundancy purposes.
 - 2.2. Backhaul going to Cable Landing Station (i.e Nasugbu, Batangas, Naic Cavite)

VIII. QUALIFICATIONS OF THE SERVICE PROVIDER

The Contractor should have the necessary eligibility, experience, and expertise in providing service the following:

A. Eligibility Requirements:

1. PhilGEPS Platinum Membership Registration Certificate/Number;
2. Mayor's/Business Permit (current and valid);
3. Tax Clearance;
4. Omnibus Sworn Statement (duly notarized); and
5. Other mandatory documents are required in Competitive Bidding under Implementing Rules and Regulations of RA No. 9184.

B. Expertise Requirements

1. At least five (5) years of experience providing Wireless Network Solutions.
2. At least ten (10) years as telephone service provider and at least ten (10) years as Internet Service Provider.
3. Must submit a Letter from the Principal Certifying Partnership, Experience, and Capability.

The contractor who has completed, within the last five (5) years from the submission and receipt of bids, a single largest contract similar to the Contract to be bid.

The prospective bidder shall also be required to include in this proposal original descriptive kinds of literature and unamended brochures of all equipment/materials to be supplied. If applicable, plans, drawings, and diagrams/configurations must likewise be provided.

The following are additional requirements which will be part of the technical bid documents:

1. All prospective bidders shall have a track record of existing installations of the offered network equipment's and structured cabling system in the Philippines.
2. The following certifications must be provided:
 - a. All prospective bidders must be authorized dealer of all equipment to be supported by certificate of dealership in the Philippines issued by the manufacturer/distributor of equipment/materials.
 - b. All prospective bidders must be capable of rendering local technical services duly certified by the manufacturer/distributor.
 - c. The bidder must have at least Three (3) Certified Licensed Electronics Engineers who are currently employed in the bidder's company trained and certified in the design and installation of Access Points. Bidder must attach certification.
 - d. Must provide 2 CCNA, 2 CCNP, 2 CCIE, and must be employed in the company.
 - e. The Bidder must be an ISO 9001:2015 and ISO 27001:2013 certified company.
 - f. The bidder provider must secure an NTC certification that they are a Tier1 Telco Company.
 - g. The bidder shall have a Fiber Optic Cable Multiplexer and shall be Gigabit Ethernet (GE) capable. Interface Hand-off: (Gigabit Ethernet 10/100/1000 - electrical)
 - h. Must have at Least 1Gbps Multi-lateral Peering with PHOpenIX for at least six (6) Years and shall Provide certification.
3. Network Requirement:
 - a. Must have at least 10 direct International Uplinks (Tier 1/Tier 2, ie. AT&T, Level 3, Telstra etc.) for redundancy purposes. Bidder shall provide detailed diagram.



- b. Must have/operate its own Backhaul going to Cable Landing Station (i.e. Nasugbu, Batangas and Naic, Cavite). Bidder shall provide detailed diagram.
 - c. Provider must have a minimum total Uplink capacity of 40Gbps (to address needs of client/s) and must provide proof therein.
 - d. Manage and operate local Internet peering (i.e. MIX, GIX, PHIX) and provide certification therein.
4. Shall submit Certificate of Employment of at least two (2) Information Technology Infrastructure Library (ITIL) Certified Engineers and shall provide proof of certification for ITIL.
 5. Shall submit network layout labeled as Electronics Engineer Plan showing connectivity from end user's data terminal facility up to the last mile duly signed by Licensed Electronics Engineer (EE) with his/her valid PRC ID.
 6. Should submit copies of Client Satisfactory Certificates from at least three (3) clients each for the last three (3) years for similar contracts.
 7. Must be an NTC registered and certified with Value Added Services (VAS) Registration license certificate.
 8. Bidders should be a certified Data Center Provider/Back up provider Tier III. Bidder shall provide proof.
 9. All prospective bidders may request the conduct a site survey and submit a report regarding the site survey.
 10. All prospective bidders shall submit their proposed Service Level Agreement (SLA) and commits to deliver and maintain their service with a Service Level Agreement of **99.8%** as stated above under the Scope of Work and provide Customer Service Center which facilitates communication between customers and various technical levels within **24 hours x 7 days a week basis**.
 11. All prospective bidders shall submit original copy of design proposal, brochures and other publications that supports compliance to the requirements.
 12. Provide and submit a proposed work plan and detailed implementation Schedule /Gantt Chart for the Project covering the whole contract period. Prospective Bidders are required to conduct site inspection. This is to ensure the reliability, security and efficiency of the required services that the contractor shall perform. Timeframe should be specified or each activity to be done and shall include Gantt Chart Summary.

Handwritten initials



Philippine Tax Academy

BIDDING DOCUMENTS

**Supply, Delivery, Installation, and Configuration of Next
Generation Firewall Appliance and Internet Dedicated Service
(IDS), and related services for the Philippine Tax Academy
(PTA)**

PUBLIC BIDDING NO. 23-08-2

Sixth Edition
July 2020




Table of Contents

Glossary of Acronyms, Terms, and Abbreviations.....	3
Section I. Invitation to Bid.....	6
Section II. Instructions to Bidders.....	10
1. Scope of Bid.....	11
2. Funding Information.....	11
3. Bidding Requirements.....	11
4. Corrupt, Fraudulent, Collusive, and Coercive Practices.....	11
5. Eligible Bidders.....	11
6. Origin of Goods.....	12
7. Subcontracts.....	12
8. Pre-Bid Conference.....	12
9. Clarification and Amendment of Bidding Documents.....	13
10. Documents comprising the Bid: Eligibility and Technical Components.....	13
11. Documents comprising the Bid: Financial Component.....	13
12. Bid Prices.....	13
13. Bid and Payment Currencies.....	14
14. Bid Security.....	14
15. Sealing and Marking of Bids.....	14
16. Deadline for Submission of Bids.....	15
17. Opening and Preliminary Examination of Bids.....	15
18. Domestic Preference.....	15
19. Detailed Evaluation and Comparison of Bids.....	15
20. Post-Qualification.....	16
21. Signing of Contract.....	16
Section III. Bid Data Sheet.....	17
Section IV. General Conditions of Contract.....	24
1. Scope of Contract.....	25
2. Advance Payment and Terms of Payment.....	25
3. Performance Security.....	25
4. Inspection and Tests.....	26
5. Warranty.....	26
6. Liability of the Supplier.....	26
Section V. Special Conditions of Contract.....	27
Section VI. Schedule of Requirements.....	32
Section VII. Technical Specification.....	34
Section VIII. Checklist of Technical and Financial Documents.....	72

Glossary of Acronyms, Terms, and Abbreviations

ABC – Approved Budget for the Contract.

BAC – Bids and Awards Committee.

Bid – A signed offer or proposal to undertake a contract submitted by a bidder in response to and in consonance with the requirements of the bidding documents. Also referred to as *Proposal* and *Tender*. (2016 revised IRR, Section 5[c])

Bidder – Refers to a contractor, manufacturer, supplier, distributor and/or consultant who submits a bid in response to the requirements of the Bidding Documents. (2016 revised IRR, Section 5[d])

Bidding Documents – The documents issued by the Procuring Entity as the bases for bids, furnishing all information necessary for a prospective bidder to prepare a bid for the Goods, Infrastructure Projects, and/or Consulting Services required by the Procuring Entity. (2016 revised IRR, Section 5[e])

BIR – Bureau of Internal Revenue.

BSP – Bangko Sentral ng Pilipinas.

Consulting Services – Refer to services for Infrastructure Projects and other types of projects or activities of the GOP requiring adequate external technical and professional expertise that are beyond the capability and/or capacity of the GOP to undertake such as, but not limited to: (i) advisory and review services; (ii) pre-investment or feasibility studies; (iii) design; (iv) construction supervision; (v) management and related services; and (vi) other technical services or special studies. (2016 revised IRR, Section 5[i])

CDA - Cooperative Development Authority.

Contract – Refers to the agreement entered into between the Procuring Entity and the Supplier or Manufacturer or Distributor or Service Provider for procurement of Goods and Services; Contractor for Procurement of Infrastructure Projects; or Consultant or Consulting Firm for Procurement of Consulting Services; as the case may be, as recorded in the Contract Form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.

CIF – Cost Insurance and Freight.

CIP – Carriage and Insurance Paid.

CPI – Consumer Price Index

DDP – Refers to the quoted price of the Goods, which means “delivered duty paid.”

DTI – Department of Trade and Industry.

EXW – Ex works.

FCA – “Free Carrier” shipping point.

FOB – “Free on Board” shipping point.

Foreign-funded Procurement or Foreign-Assisted Project– Refers to procurement whose funding source is from a foreign government, foreign or international financing institution as specified in the Treaty or International or Executive Agreement. (2016 revised IRR, Section 5[b]).

Framework Agreement – Refers to a written agreement between a procuring entity and a supplier or service provider that identifies the terms and conditions, under which specific purchases, otherwise known as “Call-Offs,” are made for the duration of the agreement. It is in the nature of an option contract between the procuring entity and the bidder(s) granting the procuring entity the option to either place an order for any of the goods or services identified in the Framework Agreement List or not buy at all, within a minimum period of one (1) year to a maximum period of three (3) years. (GPPB Resolution No. 27-2019)

GFI – Government Financial Institution.

GOCC – Government-owned and/or –controlled corporation.

Goods – Refer to all items, supplies, materials and general support services, except Consulting Services and Infrastructure Projects, which may be needed in the transaction of public businesses or in the pursuit of any government undertaking, project or activity, whether in the nature of equipment, furniture, stationery, materials for construction, or personal property of any kind, including non-personal or contractual services such as the repair and maintenance of equipment and furniture, as well as trucking, hauling, janitorial, security, and related or analogous services, as well as procurement of materials and supplies provided by the Procuring Entity for such services. The term “related” or “analogous services” shall include, but is not limited to, lease or purchase of office space, media advertisements, health maintenance services, and other services essential to the operation of the Procuring Entity. (2016 revised IRR, Section 5[r])

GOP – Government of the Philippines.

GPPB – Government Procurement Policy Board.

INCOTERMS – International Commercial Terms.

Infrastructure Projects – Include the construction, improvement, rehabilitation, demolition, repair, restoration or maintenance of roads and bridges, railways, airports, seaports, communication facilities, civil works components of information technology projects, irrigation, flood control and drainage, water supply, sanitation, sewerage and solid waste management systems, shore protection, energy/power and electrification facilities, national

buildings, school buildings, hospital buildings, and other related construction projects of the government. Also referred to as *civil works or works*. (2016 revised IRR, Section 5[u])

LGUs – Local Government Units.

NFCC – Net Financial Contracting Capacity.

NGA – National Government Agency.

PhilGEPS - Philippine Government Electronic Procurement System.

Procurement Project – refers to a specific or identified procurement covering goods, infrastructure project or consulting services. A Procurement Project shall be described, detailed, and scheduled in the Project Procurement Management Plan prepared by the agency which shall be consolidated in the procuring entity's Annual Procurement Plan. (GPPB Circular No. 06-2019 dated 17 July 2019)

PSA – Philippine Statistics Authority.

SEC – Securities and Exchange Commission.

SLCC – Single Largest Completed Contract.

Supplier – refers to a citizen, or any corporate body or commercial company duly organized and registered under the laws where it is established, habitually established in business and engaged in the manufacture or sale of the merchandise or performance of the general services covered by his bid. (Item 3.8 of GPPB Resolution No. 13-2019, dated 23 May 2019). Supplier as used in these Bidding Documents may likewise refer to a distributor, manufacturer, contractor, or consultant.

UN – United Nations.

Section I. Invitation to Bid

INVITATION TO BID FOR THE

**Supply, Delivery, Installation, and Configuration of Next Generation Firewall Appliance and Internet Dedicated Service (IDS), and related services for the Philippine Tax Academy (PTA)
Public Bidding No. 23-08-2**

The Philippine Tax Academy (PTA), through its Corporate Operating Budget FY 2023 intends to apply the sum of Twenty Million Nine Hundred Thousand Pesos (Php 20,900,000.00) being the ABC to payments under the contract for Supply, Delivery, Installation, and Configuration of Next Generation Firewall Appliance and Internet Dedicated Service (IDS) and related services for the Philippine Tax Academy (PTA)

1.

Lot No.	Quantity	Item/Description	Approved Budget for the Contract	Price of Bid Documents
1	1 lot	Next Generation Firewall Appliance	₱ 5,100,000.00	₱ 10,000.00
2	1 lot	High Availability (HA) Network Solution	₱ 8,000,000.00	₱ 15,000.00
		Internet Dedicated Services with High Availability	₱ 5,000,000.00	
		Managed Service - PABX System	₱ 1,500,000.00	
		Wireless Access Points with Cloud-based Management and Administration	₱ 800,000.00	
		Structured Cabling - Voice and Data	₱ 500,000.00	
			₱ 15,800,000.00	
Total:			₱ 20,900,000.00	₱ 25,000.00

Bids received in excess of the ABC shall be automatically rejected at bid opening.

2. The PTA, through its Bids and Awards Committee (BAC), now invites bids for the above Procurement Project. Delivery of the Goods is required by **Lot 1: Sixty (60) calendar days upon receipt of Notice to Proceed and Lot 2: Sixty (60) calendar days upon receipt of Notice to Proceed**. Bidders should have completed, within *five (5) years* from the date of submission and receipt of bids, a contract similar to the Project. The description of an eligible bidder is contained in the Bidding Documents, particularly, in Section II (Instructions to Bidders).

Summary of the bidding activities is as follows:

Advertisement/Posting of Invitation to Bid	Friday, 18 August 2023
Issuance and Availability of Bid Documents	Friday, 18 August 2023
Pre-Bid Conference	Tuesday, 29 August 2023; 10:00AM
Last Day of Request for Clarification	Friday, 01 September 2023
Last Day for Issuance of Supplemental Bid Bulletin	Tuesday, 05 September 2023
Deadline for Submission of Bids	Tuesday, 12 September 2023;10:00AM
Opening of Bids	Immediately after the Deadline for Submission of Bids

3. Bidding will be conducted through open competitive bidding procedures using a non-discretionary "*pass/fail*" criterion as specified in the 2016 revised Implementing Rules and Regulations (IRR) of Republic Act (RA) No. 9184, otherwise known as the "Government Procurement Reform Act".

Bidding is restricted to Filipino citizens/sole proprietorships, partnerships, or organizations with at least sixty percent (60%) interest or outstanding capital stock belonging to citizens of the Philippines, and to citizens or organizations of a country the laws or regulations of which grant similar rights or privileges to Filipino citizens, pursuant to RA No. 5183 and subject to Commonwealth Act 138.
4. Interested Bidders may obtain further information from the Office of the PTA and inspect the Bidding Documents through the Bids and Awards Committee (BAC) Secretariat at the address given below during 8:00 am to 5:00 pm.
5. A complete set of Bidding Documents may be acquired by interested Bidders on **18 August 2023** from the given address and website(s) below and upon payment of the applicable fee for the Bidding Documents, pursuant to the latest Guidelines issued by the GPPB, in the following amount **Lot 1: Ten Thousand Pesos (P 10,000.00) and Lot 2: Fifteen Thousand Pesos (P 15,000.00)**. The Procuring Entity shall allow the bidder to present its proof of payment for the fees in person or through electronic means.
6. The PTA will hold a Pre-Bid Conference on **29 August 2023 at 10:00 a.m.** at the **3rd Floor DOF Conference Room, DOF Building** or through video conferencing or webcasting via Google Meet which can be accessed thru this link: and shall be open to meet.google.com/edg-tqpc-ddr prospective bidders.
7. Bids must be duly received by the BAC Secretariat through manual submission at the Ground Floor, DOF Bldg., BSP Complex, Roxas Blvd., Malate, Manila, on or before **12 September 2023 at 10:00 a.m.**

Late bids shall not be accepted. Unsealed or unmarked bid envelopes shall also be rejected.
8. All Bids must be accompanied by a bid security in any of the acceptable forms and in the amount stated in ITB Clause 14.
9. Bid opening shall be on **12 September 2023 at 10:00 am** at the **3rd Floor DOF Conference Room, DOF Building**. Bids will be opened in the presence of the bidders.

representatives who choose to attend the activity.

10. Bidders shall drop their duly accomplished eligibility requirements, technical and financial proposals in two separate sealed envelopes in the designated bid box located at the at the Ground Floor, DOF Bldg., BSP Complex, Roxas Blvd., Malate, Manila.
11. The **PTA-BAC** reserves the right to reject any and all bids, declare a failure of bidding, or not award the contract at any time prior to contract award in accordance with Sections 35.6 and 41 of the 2016 revised IRR of RA No. 9184, without thereby incurring any liability to the affected bidder or bidders.
12. For further information, please refer to:

LEEANN Q. BAUTISTA
Bids and Awards Committee Secretariat
Philippine Tax Academy
7th Floor EDPC Building,
BSP Complex, Roxas Boulevard
Malate, Manila
Email: bacsec@doftaxacademy.gov.ph
Contact Number: 5317-6363 local 6200

13. You may visit the following websites:

For downloading of Bidding Documents:
<https://doftaxacademy.gov.ph>
<https://notices.philgeps.gov.ph/>

15 August 2023


ATTY. NOEMI B. ALCALA-GARCIA
BAC Chairperson

Section II. Instructions to Bidders

Notes on the Instructions to Bidders

This Section on the Instruction to Bidders (ITB) provides the information for bidders to prepare responsive bids, in accordance with the requirements of the Procuring Entity. It also provides information on bid submission, eligibility check, opening and evaluation of bids, post-qualification and on the award of contract.

1. Scope of Bid

The Procuring Entity, The Philippine Tax Academy wishes to receive Bids for the **Supply, Delivery, Installation, and Configuration of Next Generation Firewall Appliance and Internet Dedicated Service (IDS) and related services for the Philippine Tax Academy (PTA) with Public Bidding No. 23-08-2**

The Procurement Project (referred to herein as "Project") is composed of

Lot 1: Next Generation Firewall Appliance

Lot 2: High Availability (HA) Network Solution, Internet Dedicated Services (IDS) with High Availability, Managed Service - PABX System, Wireless Access Points with Cloud-based Management and Administration, and Structured Cabling - Voice and Data

the details of which are described in Section VII (Technical Specifications).

2. Funding Information

- 2.1. The GOP through the source of funding as indicated below for **FY 2023** in the amount of *Twenty Million Nine Hundred Thousand Pesos (P 20,900,000.00)*.
- 2.2. The source of funding is: **PTA Corporate Operating Budget**

3. Bidding Requirements

The Bidding for the Project shall be governed by all the provisions of RA No. 9184 and its 2016 revised IRR, including its Generic Procurement Manuals and associated policies, rules and regulations as the primary source thereof, while the herein clauses shall serve as the secondary source thereof.

Any amendments made to the IRR and other GPPB issuances shall be applicable only to the ongoing posting, advertisement, or **IB** by the BAC through the issuance of a supplemental or bid bulletin.

The Bidder, by the act of submitting its Bid, shall be deemed to have verified and accepted the general requirements of this Project, including other factors that may affect the cost, duration and execution or implementation of the contract, project, or work and examine all instructions, forms, terms, and project requirements in the Bidding Documents.

4. Corrupt, Fraudulent, Collusive, and Coercive Practices

The Procuring Entity, as well as the Bidders and Suppliers, shall observe the highest standard of ethics during the procurement and execution of the contract. They or through an agent shall not engage in corrupt, fraudulent, collusive, coercive, and obstructive practices defined under Annex "I" of the 2016 revised IRR of RA No. 9184 or other integrity violations in competing for the Project.

5. Eligible Bidders

- 5.1. Only Bids of Bidders found to be legally, technically, and financially capable will be evaluated.
- 5.2. Foreign ownership exceeding those allowed under the rules may participate pursuant:
- i. When a Treaty or International or Executive Agreement as provided in Section 4 of the RA No. 9184 and its 2016 revised IRR allow foreign bidders to participate;
 - ii. Citizens, corporations, or associations of a country, included in the list issued by the GPPB, the laws or regulations of which grant reciprocal rights or privileges to citizens, corporations, or associations of the Philippines;
 - iii. When the Goods sought to be procured are not available from local suppliers; or
 - iv. When there is a need to prevent situations that defeat competition or restrain trade.
- 5.3. Pursuant to Section 23.4.1.3 of the 2016 revised IRR of RA No.9184, the Bidder shall have an SLCC that is at least one (1) contract similar to the Project the value of which, adjusted to current prices using the PSA's CPI, must be at least equivalent to:
- Lot No. 1: The Bidder must have completed a single contract that is similar to this Project, equivalent to at least fifty percent (50%) of the ABC.**
- Lot No. 2: The Bidder must have completed a single contract that is similar to this Project, equivalent to at least fifty percent (50%) of the ABC.**
- 5.4. The Bidders shall comply with the eligibility criteria under Section 23.4.1 of the 2016 IRR of RA No. 9184.

6. Origin of Goods

There is no restriction on the origin of goods other than those prohibited by a decision of the UN Security Council taken under Chapter VII of the Charter of the UN, subject to Domestic Preference requirements under **ITB** Clause 18.

7. Subcontracts

7.1. The Procuring Entity has prescribed that: **Subcontracting is not allowed.**

8. Pre-Bid Conference

The Procuring Entity will hold a pre-bid conference for this Project on the specified date and time and either at its physical address at 3rd Floor DOF Conference Room,

DOF Building, or via Google Meet as indicated in paragraph 6 of the **IB**.

9. Clarification and Amendment of Bidding Documents

Prospective bidders may request for clarification on and/or interpretation of any part of the Bidding Documents. Such requests must be in writing and received by the Procuring Entity, either at its given address or through electronic mail indicated in the **IB**, at least *ten (10) calendar days* before the deadline set for the submission and receipt of Bids.

10. Documents comprising the Bid: Eligibility and Technical Components

- 10.1. The first envelope shall contain the eligibility and technical documents of the Bid as specified in **Section VIII (Checklist of Technical and Financial Documents)**.
- 10.2. The Bidder's SLCC as indicated in **ITB Clause 5.3** should have been completed within *five (5) years* prior to the deadline for the submission and receipt of bids.
- 10.3. If the eligibility requirements or statements, the bids, and all other documents for submission to the BAC are in foreign language other than English, it must be accompanied by a translation in English, which shall be authenticated by the appropriate Philippine foreign service establishment, post, or the equivalent office having jurisdiction over the foreign bidder's affairs in the Philippines. Similar to the required authentication above, for Contracting Parties to the Apostille Convention, only the translated documents shall be authenticated through an apostille pursuant to GPPB Resolution No. 13-2019 dated 23 May 2019. The English translation shall govern, for purposes of interpretation of the bid.

11. Documents comprising the Bid: Financial Component

- 11.1. The second bid envelope shall contain the financial documents for the Bid as specified in **Section VIII (Checklist of Technical and Financial Documents)**.
- 11.2. If the Bidder claims preference as a Domestic Bidder or Domestic Entity, a certification issued by DTI shall be provided by the Bidder in accordance with Section 43.1.3 of the 2016 revised IRR of RA No. 9184.
- 11.3. Any bid exceeding the ABC indicated in paragraph 1 of the **IB** shall not be accepted.
- 11.4. For Foreign-funded Procurement, a ceiling may be applied to bid prices provided the conditions are met under Section 31.2 of the 2016 revised IRR of RA No. 9184.

12. Bid Prices

- 12.1. Prices indicated on the Price Schedule shall be entered separately in the following manner:

- a. For Goods offered from within the Procuring Entity's country:
 - i. The price of the Goods quoted EXW (ex-works, ex-factory, ex-warehouse, ex-showroom, or off-the-shelf, as applicable);
 - ii. The cost of all customs duties and sales and other taxes already paid or payable;
 - iii. The cost of transportation, insurance, and other costs incidental to delivery of the Goods to their final destination; and
 - iv. The price of other (incidental) services, if any, listed in e.
- b. For Goods offered from abroad:
 - i. Unless otherwise stated in the **BDS**, the price of the Goods shall be quoted delivered duty paid (DDP) with the place of destination in the Philippines as specified in the **BDS**. In quoting the price, the Bidder shall be free to use transportation through carriers registered in any eligible country. Similarly, the Bidder may obtain insurance services from any eligible source country.
 - ii. The price of other (incidental) services, if any, as listed in **BDS**.

13. Bid and Payment Currencies

- 13.1. For Goods that the Bidder will supply from outside the Philippines, the bid prices may be quoted in the local currency or tradeable currency accepted by the BSP at the discretion of the Bidder. However, for purposes of bid evaluation, Bids denominated in foreign currencies, shall be converted to Philippine currency based on the exchange rate as published in the BSP reference rate bulletin on the day of the bid opening.
- 13.2. Payment of the contract price shall be made in: **Philippine Peso**.

14. Bid Security

- 14.1. The Bidder shall submit a Bid Securing Declaration¹ or any form of Bid Security in the amount indicated in the **BDS**, which shall be not less than the percentage of the ABC in accordance with the schedule in the **BDS**.
- 14.2. The Bid and bid security shall be valid until **one hundred twenty (120) calendar days from the bid opening**. Any Bid not accompanied by an acceptable bid security shall be rejected by the Procuring Entity as non-responsive.

15. Sealing and Marking of Bids

Each Bidder shall submit one copy of the first and second components of its Bid.

The Procuring Entity may request additional hard copies and/or electronic copies of the Bid. However, failure of the Bidders to comply with the said request shall not be a ground for disqualification.

If the Procuring Entity allows the submission of bids through online submission or any other electronic means, the Bidder shall submit an electronic copy of its Bid, which must be digitally signed. **An electronic copy that cannot be opened or is corrupted shall be considered non-responsive and, thus, automatically disqualified.**

16. Deadline for Submission of Bids

- 16.1. The Bidders shall submit on the specified date and time and either at its physical address or through online submission as indicated in paragraph 7 of the **IB**.

17. Opening and Preliminary Examination of Bids

- 17.1. The BAC shall open the Bids in public at the time, on the date, and at the place specified in paragraph 9 of the **IB**. The Bidders' representatives who are present shall sign a register evidencing their attendance. In case videoconferencing, webcasting or other similar technologies will be used, attendance of participants shall likewise be recorded by the BAC Secretariat.

In case the Bids cannot be opened as scheduled due to justifiable reasons, the rescheduling requirements under Section 29 of the 2016 revised IRR of RA No. 9184 shall prevail.

- 17.2. The preliminary examination of bids shall be governed by Section 30 of the 2016 revised IRR of RA No. 9184.

18. Domestic Preference

- 18.1. The Procuring Entity will grant a margin of preference for the purpose of comparison of Bids in accordance with Section 43.1.2 of the 2016 revised IRR of RA No. 9184.

19. Detailed Evaluation and Comparison of Bids

- 19.1. The Procuring BAC shall immediately conduct a detailed evaluation of all Bids rated "*passed*," using non-discretionary pass/fail criteria. The BAC shall consider the conditions in the evaluation of Bids under Section 32.2 of the 2016 revised IRR of RA No. 9184.
- 19.2. If the Project allows partial bids, bidders may submit a proposal on any of the lots or items, and evaluation will be undertaken on a per lot or item basis, as the case maybe. In this case, the Bid Security as required by **ITB Clause 15** shall be submitted for each lot or item separately.
- 19.3. The descriptions of the lots or items shall be indicated in **Section VII (Technical Specifications)**, although the ABCs of these lots or items are indicated in the

BDS for purposes of the NFCC computation pursuant to Section 23.4.2.6 of the 2016 revised IRR of RA No. 9184. The NFCC must be sufficient for the total of the ABCs for all the lots or items participated in by the prospective Bidder.

- 19.4. The Project shall be awarded as follows:
Option 2 – One Project having several items grouped into several lots, which shall be awarded as separate contracts per lot.
- 19.5. Except for bidders submitting a committed Line of Credit from a Universal or Commercial Bank in lieu of its NFCC computation, all Bids must include the NFCC computation pursuant to Section 23.4.1.4 of the 2016 revised IRR of RA No. 9184, which must be sufficient for the total of the ABCs for all the lots or items participated in by the prospective Bidder. For bidders submitting the committed Line of Credit, it must be at least equal to ten percent (10%) of the ABCs for all the lots or items participated in by the prospective Bidder.

20. Post-Qualification

- 20.1 Within a non-extendible period of five (5) calendar days from receipt by the Bidder of the notice from the BAC that it submitted the Lowest Calculated Bid, the Bidder shall submit its latest income and business tax returns filed and paid through the BIR Electronic Filing and Payment System (eFPS) and other appropriate licenses and permits required by law and stated in the **BDS**.

21. Signing of Contract

- 21.1 The documents required in Section 37.2 of the 2016 revised IRR of RA No. 9184 shall form part of the Contract. Additional Contract documents are indicated in the **BDS**.

Section III. Bid Data Sheet

Notes on the Bid Data Sheet

The Bid Data Sheet (BDS) consists of provisions that supplement, amend or specify in detail information, or requirements included in the ITB found in Section II, which are specific to each procurement.

This Section is intended to assist the Procuring Entity in providing the specific information in relation to corresponding clauses in the ITB and has to be prepared for each specific procurement.

The Procuring Entity should specify in the BDS information and requirements specific to the circumstances of the Procuring Entity, the processing of the procurement, and the bid evaluation criteria that will apply to the Bids. In preparing the BDS, the following aspects should be checked:

Information that specifies and complements provisions of the ITB must be incorporated.

Amendments and/or supplements, if any, to provisions of the ITB as necessitated by the circumstances of the specific procurement, must also be incorporated.

Bid Data Sheet

ITB Clause					
5.3	<p>For this purpose, contracts similar to the Project shall be:</p> <p>Lot 1:</p> <p>a. Similar contracts shall refer to any contract for the <i>Supply, Delivery, and Installation of Next Generation Firewall Appliance</i>.</p> <p>b. Completed within <i>Five years (5) (FYs 2019, 2020, 2021, 2022, and 2023)</i> prior to the deadline for the submission and receipt of bids.</p> <p>Lot 2:</p> <p>a. Similar contracts shall refer to any contract for the <i>Supply, Delivery, and Installation of Internet Dedicated Service (IDS) and related services</i>.</p> <p>b. Completed within <i>Five years (5) (FYs 2019, 2020, 2021, 2022, and 2023)</i> prior to the deadline for the submission and receipt of bids.</p>				
7.1	Subcontracting is not allowed.				
12	The price of the Goods shall be quoted DDP Philippine Tax Academy EDPG Building, BSP Complex, Roxas Boulevard, Malate, Manila or the applicable International Commercial Terms (INCOTERMS) for this Project.				
14.1	The bid security shall be in the form of a Bid Securing Declaration, or any of the following forms and amounts:				
	Lot No.	Item/Description	Amount Cash, Cashier's / Manager's Check, Bank Draft/ Guarantee/ Irrevocable Letter of Credit (2%)	Surety bond callabe upon demand issued by a surety or insurance company duly certifid by the Insurance Comission (5%)	Bid Securing Declaration (Pursuant to GPPB Resolution No. 03- 2012)
	1	Next Generation Firewall Appliance	P 102,000.00	P 255,000.00	Please see Section VIII attached as Annex "F"
	2	High Availability (HA) Network Solution, Internet Dedicated Services (IDS) with High	P 316,000.00	P 790,000.00	

		Availability, Managed Service - PABX System, Wireless Access Points with Cloud- based Management and Administratio n and Structured Cabling - Voice and Data			
		<p>The bid security in the form of cashier's/manager's check shall be payable to the PHILIPPINE TAX ACADEMY.</p>			
15	<p>Sealing and Marking of Envelopes: Each bidder must submit two (2) copies of the technical and financial components of its bid: one (1) original and/or certified copy of the original documents and (1) photocopies thereof.</p>				

Original eligibility and technical documents shall be enclosed in one sealed envelope and the original financial component in another sealed envelope containing the markings:

TECHNICAL COMPONENT
SUPPLY, DELIVERY, INSTALLATION, AND CONFIGURATION
OF NEXT-GENERATION FIREWALL APPLIANCE AND INTERNET DEDICATED
SERVICE (IDS) AND RELATED SERVICES FOR THE PHILIPPINE TAX ACADEMY
(PTA)

(COMPANY NAME)
(COMPANY ADDRESS)
(E-MAIL ADDRESS & TELEPHONE NUMBER)

ATTY. NOEMI B. ALCALA-GARCIA
CHAIRPERSON
PHILIPPINE TAX ACADEMY BIDS AND AWARDS COMMITTEE
ROXAS BOULEVARD, MANILA

PUBLIC BIDDING NO. 2023-08-2
DO NOT OPEN BEFORE: 12 SEPTEMBER 2023, 10:00 AM

FINANCIAL COMPONENT
SUPPLY, DELIVERY, INSTALLATION, AND CONFIGURATION
OF NEXT-GENERATION FIRE WALL APPLIANCE AND INTERNET DEDICATED
SERVICE (IDS) AND RELATED SERVICES FOR THE PHILIPPINE TAX ACADEMY
(PTA)

(COMPANY NAME)
(COMPANY ADDRESS)
(E-MAIL ADDRESS & TELEPHONE NUMBER)

ATTY. NOEMI B. ALCALA-GARCIA
CHAIRPERSON
PHILIPPINE TAX ACADEMY BIDS AND AWARDS COMMITTEE
ROXAS BOULEVARD, MANILA

PUBLIC BIDDING NO. 2023-08-2
DO NOT OPEN BEFORE: 12 SEPTEMBER 2023, 10:00 AM

The envelopes containing the original and the copies shall then be enclosed in one single envelope containing the following markings:

All envelopes shall then be enclosed in a main envelope containing the markings:

SUPPLY, DELIVERY, INSTALLATION, AND CONFIGURATION
OF NEXT GENERATION FIREWALL APPLIANCE AND INTERNET DEDICATED
SERVICE (IDS) AND RELATED SERVICES FOR THE PHILIPPINE TAX ACADEMY
(PTA)

(COMPANY NAME)
(COMPANY ADDRESS)
(E-MAIL ADDRESS & TELEPHONE NUMBER)

ATTY. NOEMI B. ALCALA-GARCIA
CHAIRPERSON
PHILIPPINE TAX ACADEMY BIDS AND AWARDS COMMITTEE
ROXAS BOULEVARD, MANILA

PUBLIC BIDDING NO. 2023-08-2
DO NOT OPEN BEFORE: 12 SEPTEMBER 2023, 10:00 AM

19.3	<p>The NFCC computation, if applicable, must be sufficient for all the lots or contracts to be awarded to the Bidder:</p> <table border="1" data-bbox="418 386 1334 1150"> <thead> <tr> <th data-bbox="418 386 548 491">Lot No.</th> <th data-bbox="548 386 776 491">Quantity</th> <th data-bbox="776 386 1123 491">Item/Description</th> <th data-bbox="1123 386 1334 491">Approved Budget for the Contract</th> </tr> </thead> <tbody> <tr> <td data-bbox="418 491 548 596">1</td> <td data-bbox="548 491 776 596">1</td> <td data-bbox="776 491 1123 596">Next Generation Firewall Appliance</td> <td data-bbox="1123 491 1334 596">P5,100,000.00</td> </tr> <tr> <td data-bbox="418 596 548 1058">2</td> <td data-bbox="548 596 776 1058">1</td> <td data-bbox="776 596 1123 1058">High Availability (HA) Network Solution, Internet Dedicated Services with High Availability, Managed Service - PABX System, Wireless Access Points with Cloud-based Management and Administration, and Structured Cabling - Voice and Data</td> <td data-bbox="1123 596 1334 1058">P15,800,000.00</td> </tr> <tr> <td data-bbox="418 1058 548 1150"></td> <td data-bbox="548 1058 776 1150"></td> <td data-bbox="776 1058 1123 1150" style="text-align: right;">Total ABC:</td> <td data-bbox="1123 1058 1334 1150">P20,900,000.00</td> </tr> </tbody> </table>	Lot No.	Quantity	Item/Description	Approved Budget for the Contract	1	1	Next Generation Firewall Appliance	P5,100,000.00	2	1	High Availability (HA) Network Solution, Internet Dedicated Services with High Availability, Managed Service - PABX System, Wireless Access Points with Cloud-based Management and Administration, and Structured Cabling - Voice and Data	P15,800,000.00			Total ABC:	P20,900,000.00
Lot No.	Quantity	Item/Description	Approved Budget for the Contract														
1	1	Next Generation Firewall Appliance	P5,100,000.00														
2	1	High Availability (HA) Network Solution, Internet Dedicated Services with High Availability, Managed Service - PABX System, Wireless Access Points with Cloud-based Management and Administration, and Structured Cabling - Voice and Data	P15,800,000.00														
		Total ABC:	P20,900,000.00														
20.2	<p>For purposes of Post-qualification within a non-extendible period of five (5) calendar days from receipt by the Bidder of notice from the BAC that it had submitted the LCB, the Bidder shall submit the following documentary requirements:</p> <ol style="list-style-type: none"> 1. Income Tax Returns for year 2022 (BIR Form 1701 or 1702). 2. Latest Value Added Tax Returns (Forms 2550M and 2550Q) or Percentage Tax Returns (Form 2551M). For this requirement, covering the last six (6) months prior to the Opening of Bids. <p><i>The income tax and business tax returns stated above should have been filed through the Electronic Filing and Payment System (EFPS). However, exceptions issued by the BIR are recognized (i.e. BIR RMC No. 4-2021) subject to validation and verification.</i></p> <ol style="list-style-type: none"> 3. BIR Tax Registration Certificate (BIR Form 2303) 4. Proof of completion of the single largest contract as identified in the Statement of Single Largest Contract, which shall be copy of any 																

	<p>verifiable document(s) such as but not limited to the following:(a) Contract/s or Purchase Order/s; (b) corresponding Sales Invoice/s; (c) Official Receipt/Cash Receipt/Collection Receipt; and (d) Certificate of Satisfactory Completion.</p> <p>5. Submission of proof of evidence as proof of compliance with the bidder's actual offer, if applicable.</p> <p style="padding-left: 40px;">a. Brochure or Technical Data Sheet</p> <p>In the column "Bidder's Compliance", the bidder must state "comply" against each of the individual parameters of each specification corresponding to performance parameter of equipment offered. Statement of "comply" must be supported by evidence in a bidders bid and cross-referenced to that evidence. Evidence shall be in the form of manufacturer's or distributor's un-amended sales literature, unconditional statements or specification and compliance issued by the manufacturer or distributor, samples, independent test data etc., as appropriate.</p>
21.1	<p>The winning bidder shall post the required Performance Security and enter into contract with the Procuring Entity within ten (10) calendar days from receipt by the winning bidder of the Notice of Award.</p>

Section IV. General Conditions of Contract

Notes on the General Conditions of Contract

The General Conditions of Contract (GCC) in this Section, read in conjunction with the Special Conditions of Contract in Section 5 and other documents listed therein, should be a complete document expressing all the rights and obligation of the parties.

Matters governing performance of the Supplier, payments under the contract, or matters affecting the risks, rights, and obligations of the parties under the contract are include in the GCC and Special Conditions of Contract.

Any complementary information, which may be needed, shall be introduced only through the Special Conditions of Contract.

1. Scope of Contract

This Contract shall include all such items, although not specifically mentioned, that can be reasonably inferred as being required for its completion as if such items were expressly mentioned herein. All the provisions of RA No. 9184 and its 2016 revised IRR, including the Generic Procurement Manual, and associated issuances, constitute the primary source for the terms and conditions of the Contract, and thus, applicable in contract implementation. Herein clauses shall serve as the secondary source for the terms and conditions of the Contract.

This is without prejudice to Sections 74.1 and 74.2 of the 2016 revised IRR of RA No. 9184 allowing the GPPB to amend the IRR, which shall be applied to all procurement activities, the advertisement, posting, or invitation of which were issued after the effectivity of the said amendment.

Additional requirements for the completion of this Contract shall be provided in the **Special Conditions of Contract (SCC)**.

2. Advance Payment and Terms of Payment

- 2.1 Advance payment of the contract amount is provided under Annex "D" of the revised 2016 IRR of RA No. 9184.
- 2.2 The Procuring Entity is allowed to determine the terms of payment on the partial or staggered delivery of the Goods procured, provided such partial payment shall correspond to the value of the goods delivered and accepted in accordance with prevailing accounting and auditing rules and regulations. The terms of payment are indicated in the SCC.

3. Performance Security

Within ten (10) calendar days from receipt of the Notice of Award by the Bidder from the Procuring Entity but in no case later than prior to the signing of the Contract by both parties, the successful Bidder shall furnish the performance security in any of the forms prescribed in Section 39 of the 2016 revised IRR of RA No. 9184.

4. Inspection and Tests

The Procuring Entity or its representative shall have the right to inspect and/or to test the Goods to confirm their conformity to the Project specifications at no extra cost to the Procuring Entity in accordance with the Generic Procurement Manual. In addition to tests in the SCC, **Section IV (Technical Specifications)** shall specify what inspections and/or tests the Procuring Entity requires, and where they are to be conducted. The Procuring Entity shall notify the Supplier in writing, in a timely manner, of the identity of any representatives retained for these purposes.

All reasonable facilities and assistance for the inspection and testing of Goods, including access to drawings and production data, shall be provided by the Supplier to the authorized inspectors at no charge to the Procuring Entity.

5. Warranty

- 5.1 In order to assure that manufacturing defects shall be corrected by the Supplier, a warranty shall be required from the Supplier as provided under Section 62.1 of the 2016 revised IRR of RA No. 9184.
- 5.2 The Procuring Entity shall promptly notify the Supplier in writing of any claims arising under this warranty. Upon receipt of such notice, the Supplier shall, repair or replace the defective Goods or parts thereof without cost to the Procuring Entity, pursuant to the Generic Procurement Manual.

6. Liability of the Supplier

The Supplier's liability under this Contract shall be as provided by the laws of the Republic of the Philippines.

If the Supplier is a joint venture, all partners to the joint venture shall be jointly and severally liable to the Procuring Entity.

Section V. Special Conditions of Contract

Notes on the Special Conditions of Contract

Similar to the BDS, the clauses in this Section are intended to assist the Procuring Entity in providing contract-specific information in relation to corresponding clauses in the GCC found in Section IV.

The Special Conditions of Contract (SCC) complement the GCC, specifying contractual requirements linked to the special circumstance of the Procuring Entity, the Procuring Entity's country, the sector, and the Goods purchased. In preparing this Section, the following aspects should be checked:

Information that complements provisions of the GCC must be incorporated.

Amendments and/or supplements to provisions of the GCC as necessitated by the circumstances of the specific purchase, must also be incorporated.

However, no special conditions which defeats or negates the general intent and purpose of the provisions of the GCC should be incorporated herein.

Special Conditions of Contract

GCC Clause	
1	<p style="text-align: center;">Delivery and Documents –</p> <p>For purposes of the Contract, “EXW,” “FOB,” “FCA,” “CIF,” “CIP,” “DDP” and other trade terms used to describe the obligations of the parties shall have the meanings assigned to them by the current edition of INCOTERMS published by the International Chamber of Commerce, Paris. The Delivery terms of this Contract shall be as follows:</p> <p>The delivery terms applicable to this Contract are delivered <i>at Philippine Tax Academy (PTA), EDPC Building, BSP Complex, Roxas Boulevard, Malate, Manila</i>. Risk and title will pass from the Supplier to the Procuring Entity upon receipt and final acceptance of the Goods at their final destination.”</p> <p>Delivery of the Goods shall be made by the Supplier in accordance with the terms specified in Section VI (Schedule of Requirements).</p> <p>For purposes of this Clause the Procuring Entity’s Representative at the Project Site is <i>Ms. Leann Q. Bautista</i>.</p> <p>Incidental Services –</p> <p>The Supplier is required to provide all of the following services, including additional services, if any, specified in Section VI, Schedule of Requirements:</p> <ul style="list-style-type: none"> b. performance or supervision of on-site assembly and/or start-up of the supplied Goods; c. furnishing of tools required for assembly and/or maintenance of the supplied Goods; d. furnishing of a detailed operations and maintenance manual for each appropriate unit of the supplied Goods; e. performance or supervision or maintenance and/or repair of the supplied Goods, for a period of time agreed by the parties, provided that this service shall not relieve the Supplier of any warranty obligations under this Contract; and f. training of the Procuring Entity’s personnel, at the Supplier’s plant and/or on-site, in assembly, start-up, operation, maintenance, and/or repair of the supplied Goods.

The Contract price for the Goods shall include the prices charged by the Supplier for incidental services and shall not exceed the prevailing rates charged to other parties by the Supplier for similar services.

Spare Parts –

The Supplier is required to provide all of the following materials, notifications, and information pertaining to spare parts manufactured or distributed by the Supplier:

- a. such spare parts as the Procuring Entity may elect to purchase from the Supplier, provided that this election shall not relieve the Supplier of any warranty obligations under this Contract; and
- b. in the event of termination of production of the spare parts:
 - i. advance notification to the Procuring Entity of the pending termination, in sufficient time to permit the Procuring Entity to procure needed requirements; and
 - ii. following such termination, furnishing at no cost to the Procuring Entity, the blueprints, drawings, and specifications of the spare parts, if requested.

The spare parts and other components required are listed in **Section VI (Schedule of Requirements)** and the cost thereof are included in the contract price.

The Supplier shall carry sufficient inventories to assure ex-stock supply of consumable spare parts or components for the Goods for a period of *three (3) months*.

Spare parts or components shall be supplied as promptly as possible, but in any case, within *three (3) months* of placing the order.

	<p>Packaging –</p> <p>The Supplier shall provide such packaging of the Goods as is required to prevent their damage or deterioration during transit to their final destination, as indicated in this Contract. The packaging shall be sufficient to withstand, without limitation, rough handling during transit and exposure to extreme temperatures, salt and precipitation during transit, and open storage. Packaging case size and weights shall take into consideration, where appropriate, the remoteness of the Goods' final destination and the absence of heavy handling facilities at all points in transit.</p> <p>The packaging, marking, and documentation within and outside the packages shall comply strictly with such special requirements as shall be expressly provided for in the Contract, including additional requirements, if any, specified below, and in any subsequent instructions ordered by the Procuring Entity.</p> <p>The outer packaging must be clearly marked on at least (4) sides as follows:</p> <ul style="list-style-type: none"> Name of the Procuring Entity Name of the Supplier Contract Description Final Destination Gross Weight Any special lifting instructions Any special handling instructions Any relevant HAZCHEM classifications
	<p>A packaging list identifying the contents and quantities of the package is to be placed on an accessible point of the outer packaging if practical. If not practical the packaging list is to be placed inside the outer packaging but outside the secondary packaging.</p> <p>Transportation –</p> <p>Where the Supplier is required under Contract to deliver the Goods CIF, CIP, or DDP, transport of the Goods to the port of destination or such other named place of destination in the Philippines, as shall be specified in this Contract, shall be arranged and paid for by the Supplier, and the cost thereof shall be included in the Contract Price.</p> <p>Where the Supplier is required under Contract to deliver the Goods CIF, CIP or DDP, Goods are to be transported on carriers of Philippine registry. In the event that no carrier of Philippine registry is available, Goods may be shipped by a carrier which is not of Philippine registry provided that the Supplier obtains and presents to the Procuring Entity certification to this effect from the nearest Philippine consulate to the port of dispatch. In the event that carriers of Philippine registry are available but their schedule delays the Supplier in its</p>

	<p>performance of this Contract the period from when the Goods were first ready for shipment and the actual date of shipment the period of delay will be considered force majeure.</p> <p>The Procuring Entity accepts no liability for the damage of Goods during transit other than those prescribed by INCOTERMS for DDP deliveries. In the case of Goods supplied from within the Philippines or supplied by domestic Suppliers risk and title will not be deemed to have passed to the Procuring Entity until their receipt and final acceptance at the final destination.</p> <p>Intellectual Property Rights –</p> <p>The Supplier shall indemnify the Procuring Entity against all third-party claims of infringement of patent, trademark, or industrial design rights arising from use of the Goods or any part thereof.</p>
2.2	Payment will be made upon complete acceptance of the project.
4	The inspections and tests will be conducted by the Inspection and Acceptance Committee of Philippine Tax Academy and the end-user

Section VI. Schedule of Requirements

The delivery schedule expressed as weeks/months stipulates hereafter a delivery date which is the date of delivery to the project site.

Lot No.	Description	Quantity	Total	Delivered, Weeks/Months
1	Next Generation Firewall Appliance	1 lot	1 lot	Within 60 calendar days upon receipt of Notice to proceed (NTP)

I hereby certify to comply and deliver all of the above requirements in accordance with the above stated schedule.

Name of Agency

Signature over Printed Name
of the Authorized Representative

Date

Section VI. Schedule of Requirements

The delivery schedule expressed as weeks/months stipulates hereafter a delivery date which is the date of delivery to the project site.

Lot No.	Description	Quantity	Total	Delivered, Weeks/Months
2	High Availability (HA) Network Solution	1 lot	1 lot	Within 60 calendar days upon receipt of Notice to proceed (NTP)
	Internet Dedicated Services with High Availability.			
	Managed Service - PABX System			
	Wireless Access Points with Cloud-based Management and Administration			
	Structured Cabling - Voice and Data			

I hereby certify to comply and deliver all of the above requirements in accordance with the above stated schedule.

Name of Agency

Signature over Printed Name
of the Authorized Representative

Date

Section VII. Technical Specification

Notes for Preparing the Technical Specifications

A set of precise and clear specifications is a prerequisite for Bidders to respond realistically and competitively to the requirements of the Procuring Entity without qualifying their Bids. In the context of Competitive Bidding, the specifications (e.g. production/delivery schedule, manpower requirements, and after-sales service/parts, descriptions of the lots or items) must be prepared to permit the widest possible competition and, at the same time, present a clear statement of the required standards of workmanship, materials, and performance of the goods and services to be procured. Only if this is done will the objectives of transparency, equity, efficiency, fairness and economy in procurement be realized, responsiveness of bids be ensured, and the subsequent task of bid evaluation and post-qualification facilitated. The specifications should require that all items, materials and accessories to be included or incorporated in the goods be new, unused, and of the most recent or current models, and that they include or incorporate all recent improvements in design and materials unless otherwise provided in the Contract.

Samples of specifications from previous similar procurements are useful in this respect. The use of metric units is encouraged. Depending on the complexity of the goods and the repetitiveness of the type of procurement, it may be advantageous to standardize the General Technical Specifications and incorporate them in a separate subsection. The General Technical Specifications should cover all classes of workmanship, materials, and equipment commonly involved in manufacturing similar goods. Deletions or addenda should then adapt the General Technical Specifications to the particular procurement.

Care must be taken in drafting specifications to ensure that they are not restrictive. In the specification of standards for equipment, materials, and workmanship, recognized Philippine and international standards should be used as much as possible. Where other particular standards are used, whether national standards or other standards, the specifications should state that equipment, materials, and workmanship that meet other authoritative standards, and which ensure at least a substantially equal quality than the standards mentioned, will also be acceptable. The following clause may be inserted in the Special Conditions of Contract or the Technical Specifications.

Sample Clause: Equivalency of Standards and Codes

Wherever reference is made in the Technical Specifications to specific standards and codes to be met by the goods and materials to be furnished or tested, the provisions of the latest edition or revision of the relevant standards and codes shall apply, unless otherwise expressly stated in the Contract. Where such standards and codes are national or relate to a particular country or region, other authoritative standards that ensure substantial equivalence to the standards and codes specified will be acceptable.

Reference to brand name and catalogue number should be avoided as far as possible; where unavoidable they should always be followed by the words "or at least equivalent." References to brand names cannot be used when the funding source is the GOP.

Where appropriate, drawings, including site plans as required, may be furnished by the Procuring Entity with the Bidding Documents. Similarly, the Supplier may be requested to provide drawings or samples either with its Bid or for prior review by the Procuring Entity during contract execution.

Bidders are also required, as part of the technical specifications, to complete their statement of compliance demonstrating how the items comply with the specification.

Section VII: Technical Specifications

LOT NO. 1	Next Generation Firewall Appliance
QUANTITY	1 Lot

AGENCY SPECIFICATIONS	BIDDER'S STATEMENT OF COMPLIANCE ¹¹
	Brand and Model:
Next Generation Firewall Appliance with Three (3) year Warranty on Hardware Appliance, Licenses and Support Services.	
Configuration, Implementation and installation Services	
Knowledge Transfer Training	
The proposed Next Generation Firewall must support the following:	
1. Hardware:	
1.1 Not lower than 6.8 Gbps of Firewall Throughput.	
1.2 Nine hundred forty-five thousand 945,000 maximum sessions and at least One hundred thousand 100,000 new sessions per second.	
1.3 Not lower than 3.2 Gbps of Threat Prevention throughput.	
1.4 Not lower than 4.6 Gbps of Internet Protocol Security (IPSEC) Virtual Private Network (VPN) throughput.	
1.5 12 x RJ-45 10/100/1000Mbps ports for network traffic.	
1.6 High-Availability (HA) both Active/Active and Active/Passive modes.	
1.7 Fully redundant power supply with an additional power supply module	
1.8 Not lower than 120 GB SSD disk drive capacity.	

¹¹ Bidders must state here either "Comply" or "Not Comply" against each of the individual parameters of each Specification stating the corresponding performance parameter of the equipment offered. Statements of "Comply" or "Not Comply" must be supported by evidence in a Bidder's Bid and cross-referenced to that evidence. Evidence shall be in the form of manufacturer's un-amended sales literature, unconditional statements of specification and compliance issued by the manufacturer, samples, independent test data etc., as appropriate. A statement that is not supported by evidence or is subsequently found to be contradicted by the evidence presented will render the Bid under evaluation liable for rejection. A statement either in the Bidder's statement of compliance or the supporting evidence that is found to be false either during Bid evaluation, post-qualification or the execution of the Contract may be regarded as fraudulent and render the Bidder or supplier liable for prosecution subject to the applicable laws and issuances.

13

2.Functional Requirements:	
2.1 The Proposed Next-Generation Firewall must have a separate and dedicated CPU, Memory, and Hard drive for the control plane and data plane. To avoid service interruption on the data processing plane when the control plane has been restarted or rebooted.	
2.2 A hardened Operating System (OS) must be built as a firewall appliance and not built from generic server hardware.	
2.3 Must handle all traffic in a single pass stream-based manner with all security features turned on to deliver predictable performance. It shall be optimized for Layer Seven (7) application-level content processing to handle signature matching and processing in a single-pass parallel processing architecture.	
2.4 Must have a basic malware analysis service without any additional subscription. The firewall should forward portable executable files to the malware analysis service for analysis.	
2.5 Must offer safe application enablement capabilities to build firewall policies based on application/application features, users and groups, and content, as opposed to port, protocol, and IP address, transforming your traditional allow or deny firewall policy into business-friendly elements.	
2.6 Must support application detection, which determines what an application is irrespective of port, protocol, encryption Secure Shell or Secure Sockets Layer (SSH or SSL), or any other evasive tactic the application uses. The solution must support multiple classification mechanisms such as application signatures, application protocol decoding, and heuristics to your network traffic stream to accurately identify applications.	
2.7 Must support dynamic addition of workload into a dynamic address object. Any additional workload into a pool of servers belonging to a dynamic address object will automatically apply the corresponding security policy without manual intervention.	
2.8 Must natively support decryption of Transport Layer Security (TLS) 1.3 without downgrading to TLS 1.2	
2.9 Must provide enhanced reporting and logging of decrypted and encrypted traffic.	
2.10 Must be able to integrate to an external web server Hypertext Transfer Protocol Secure (HTTPS) containing dynamic IP, Uniform Resource Locators (URL), or Domain list(s) that can be referenced for security policy (e.g., whitelisting or blacklisting purposes). Any changes on the list should be dynamically captured and automatically applied to the security policy without manual intervention.	

2.11 It must have an interactive and customizable graphical summary of the applications, users, URLs, threats, and content traversing the network it protects.	
2.12 Must provide a unified view of logs and separate detailed logs for each type (e.g., traffic, URL, threats, file analysis, system, configuration, users, etc.) for easy analysis.	
2.13 Must be able to natively trigger custom alerts/logs based on conditions produced by different event sources (e.g., traffic, threat, URL, system, configuration) and forward customizable attribute value via HTTP-based service that exposes an Application Programming Interface (API) (via HTTPS), email Simple Mail Transfer Protocol (SMTP), Syslog and Simple Network Management Protocol (SNMP) Trap.	
2.14 Must have native built-in functionality to auto quarantine or blacklist IP addresses to existing security policies based on any log attributes from multiple log sources (e.g., traffic, threat, URL, etc.).	
3.Certification / Accreditation / Awards	
3.1 The proposed solution must be in the leader's quadrant position of Gartner Magic Quadrant for Enterprise Network Firewall. (Must be verifiable thru Gartner's Website)	
3.2 The proposed solution must be from a security vendor that is part of the leader category in the Forrester Wave Zero Trust extended Ecosystem Platform Providers to support PTA towards a Zero Trust framework. (Must be verifiable thru Forrester's Website or Principal's website)	
3.3 The cloud-based malware analysis platform of the proposed solution must have SOC2 Type II Plus certification. (Must be verifiable thru Principal's website).	
4.Local Management	
4.1 The proposed Next Generation Firewall must be fully configurable and manageable using a Web-based Graphical User Interface (GUI) via a standard Web Browser (HTTP) and/or Command Line Interface (CLI) via Secure Shell (SSH) application. No additional client software shall be required to configure security policies, objects, etc.	
4.2 The proposed solution, if managed by a Central Management System, must be able to add, edit or remove firewall policies that are locally created. The FW appliance will allow flexibility when the Central Management System (CMS) is down/unreachable or security policies are applicable only to specific Virtual Next Generation Security Firewalls.	
4.3 Must generate local reports on a manual ad-hoc or schedule (daily, weekly, monthly, etc.) without additional software subscription/licenses or hardware components.	

4.4 Must log all administrative activities on the web and the command line interface.	
4.5 Must be able to assign management functions for each user or group granularly defined Role Based Access Control (RBAC).	
4.6 Must support Extensible Markup Language (XML) Application Programming Interface (API) that allows other systems to manage/integrate with the solution.	
4.7 Must have a native policy optimization tool to help effectively migrate from traditional/legacy port protocol to application-based rules. It must have usage tracking of the actual application for every security policy that utilizes Port Based Rules (PBR).	
4.8 Must have a native policy optimization tool that can help identify unused security policies. It must not be limited to policy hit count and must have policy rule usage analysis based on an adjustable time frame.	
4.9 Must have a native policy optimization tool to help track and fix overly permissive security policies (allow any port/application).	
4.10 Must have tagging or labeling capability attached to security policies and objects for automation and policy management optimization.	
4.11 It must have a global search function that allows the security admins to search for policy names and objects across your entire configuration	
5. Threat Prevention	
5.1 The proposed solution must inspect all traffic for threats, regardless of port and protocol, and automatically blocks known vulnerabilities, malware, exploits, spyware, and Command-and-Control (C&C).	
5.2 For the encrypted traffic Secure Socket Layer (SSL), the proposed solution must be able to selectively apply a policy-based decryption and then inspect the traffic for threats, regardless of ports.	
5.3 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.	
5.4 The security platform must support an external dynamic list where it offers the capability to ingest multiple feeds from third-party Indicators of Compromise (IOCs) feeds on IP addresses, URLs, or Domains, then can be automated into policy enforcement to deny/reset/drop the matching traffic. If yes, please provide evidence to support the statement.	
5.5 Must support packet capturing of specific threats for forensic evidence or investigation.	
5.6 It must provide the ability to allow the organization to write its customized threat signatures for new or	

targeted threats that may not be found in other environments.	
5.7 Must be able to define different antivirus/vulnerability protection / antispymware security profiles for each security policy defined.	
6.Domain Name System (DNS) Security	
6.1 The proposed solution must stop known and unknown DNS traffic with Machine Learning (ML) and predictive analytics.	
6.2 Must help identify systems that are infected/compromised by sink holing DNS requests to a command and control server	
6.3 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 C&C server. In addition, it should identify DGA domains based on dictionary words.	
6.4 Protect against DNS Tunneling-based attacks that utilize crafted DNS queries and responses to hide malware delivery, C&C traffic, or data exfiltration/extraction.	
6.5 Must protect against ultra-low/slow DNS tunnels that spread tunneled data and exploits across multiple domains and use prolonged rates to evade detection, steal data, or send additional malicious payloads into your network.	
6.6 Must protect against strategically aged domains using predictive analytics. It should protect users from connecting to reserved domains and left dormant for months before use by malicious actors.	
6.7 It must prevent fast flux, a technique cybercriminals use to cycle through bots and DNS records. Fast flux networks are used for phishing, malware distribution, scams, and botnet operations.	
6.8 Must protect against domains surreptitiously added to hacked DNS zones of reputable domains.	
6.9 Must prevent DNS rebinding attacks, which can be used to move laterally and attack services inside the corporate network from the internet.	
6.10 Must prevent dangling DNS attacks, which use stale DNS zone data to take over domains and cause reputational harm or launch phishing attacks.	
6.11 Must support the following DNS Security Categories:	
<ul style="list-style-type: none"> • Command and Control (C2) or (C&C) • Dynamic DNS (DDNS) • Malware 	
<ul style="list-style-type: none"> • Newly Registered Domains • Phishing 	

<ul style="list-style-type: none"> • Grayware • Parked <p>Proxy Avoidance & Anonymizers</p>	
7.Advanced Uniform Resource Locators (URL) Filtering	
7.1 Must have natively-integrated URL filtering capabilities.	
7.2 Must support locally defined URL entries/categories.	
7.3 Must have an automated cloud-based dynamic URL categorization for classifying unknown websites.	
7.4 Must have a specific category for Malware, Phishing, Command-and-Control, Proxy Avoidance, and Anonymizers, among other usual web categories.	
7.5 Must support multi-category URL filtering capabilities that include risk categories for more granular URL categorization.	
7.6 Must have Inline (Machine Learning) 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).	
7.7 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 (CAPTCHAs), and Hypertext Markup Language (HTML) character encoding.	
7.8 Must have real-time detection and prevention of credential theft by controlling sites where users can submit corporate credentials based on the site's URL category.	
7.9 Must have phishing image detection that uses ML models to analyze images on web pages to determine whether they are imitating brands commonly used in phishing attempts.	
7.10 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). - Except for government, banking institution, and healthcare provider URL categories from decryption.	
8.Advanced Threat Analysis	
8.1 The proposed solution must identify unknown malware using a cloud-based malware analysis platform with advanced detection capabilities like Static & Dynamic Analysis, Bare-metal analysis, Machine Learning, Dynamic unpacking, Network Traffic profiling, and Recursive Analysis.	

✓

8.2 The proposed cloud-based malware analysis platform must have Security Operations Center (SOC)2 Type II Plus Certification.	
8.3 Must support automatic creation and delivery of protection signatures from locally submitted samples and dynamic updates from the platform.	
8.4 The proposed cloud-based malware analysis platform must have a custom-built hypervisor that detects and analyze evasive attacks.	
8.5 Must be able to identify and prevent variants of known malware Portable Executable (PE and PowerShell file types) in real-time using the local machine learning module.	
8.6 Must have a machine learning module that is updated automatically in the form of training sets from the cloud-based advanced malware analysis platform.	
9.Warranty, Support and Service Level Agreement (SLA)	
9.1 The proposed solution must include 3 Years Warranty on the following Licenses, Appliance, and Support services: <ul style="list-style-type: none"> • Hardware Appliance • Advance Threat Prevention • DNS Security • Advance URL Filtering • Advance Wildfire Protection SDWAN 	
9.2 Service Level Agreement SLA <ul style="list-style-type: none"> • 24x7 Helpdesk Support • 8x5x nbd (next business day) with parts and onsite service support for appliance and configurations during the warranty period. • Must provide service unit in case of appliance failure or errors within 48 hours from when the incident is reported. 	
10. Additional Requirements	
10.1 The Supplier must have at least two (2) Certified Network Security Engineer of the proposed solution and must be employed in the company for at least 2 years. (must provide copy of Engineers Certification from the manufacturer and Certificate of Employment, Company – ID, and Resume/CV).	
10.2 The Supplier must submit Manufacturer/Principal Authorization Certification of the proposed Solution.	
10.3 The Supplier must be at least twenty (20) years in the IT Industry.	

Scope of Work:
Supply, delivery, installation and configuration of Next Generation Firewall Appliance (NGFW).

The deployment task includes the following:

1. Project Kick-Off
2. The winning bidder will provide Network Topology Design and Documentation.
3. The winning bidder will perform the following tasks to install and configure a Next-Generation Firewall:
 - 3.1. Installation of NGFW Appliance in PTA's network environment (includes mounting to PTA rack, power supply, and fan trays if applicable.)
 - 3.2. Update NGFW to latest firmware, and activate licenses support and subscription (Advance Threat Prevention, DNS Security, Advance URL Filtering, Advance Threat Analysis, etc.)
 - 3.3. Configure Firewall policies, NAT configuration, Zones, Routes, Services, Objects, VLANs, IP addresses, interfaces, and test basic routing capabilities.
 - 3.4. Configure WAN connectivity, WAN Fallover, SSL Decryption, SSL VPN, IPsec VPN(Site to site) and syslog.
 - 3.5. Perform functionality testing of internal and external application/servers.
 - 3.6. Prevent customer's server and user for attacks and Intrusion
 - 3.7. Assess and review the routes for each network traffic
 - 3.8. Discover business needs for network and security distribution
 - 3.9. Burn-test NGFW Appliance for 24 hours.
4. Activate licenses support and subscription features (URL Filtering, Threat Prevention, and Wildfire)
5. The winning bidder will implement User-ID or IP-Base security function in the PTA Domain as defined in the design documentation.
6. The winning bidder will provide User-ID to IP mapping. Tasks will include:
 - 6.1. Map User-ID to IP address information for the number of Authentication domains as defined in the design.

<ul style="list-style-type: none"> 6.2. Collect User Group information per defined authentication domain. 6.3. Requirements review and definition of User domain environments. 6.4. Use of system logs to gather User and IP address information. 7. The winning bidder will implement App-ID functionality in the Targeted Network/Policy. <ul style="list-style-type: none"> 7.1. Convert all well-known applications from Port-based rules to application-based policies. 7.2. Isolate all unknown TCP/UDP traffic rules. 7.3. Finalize and modify App-ID policy on a third scan performed at agreed scheduled time, subsequent to completion of the second App-ID scan. 7.4. Remove Port-based rules. 8. The winning bidder will configure Advance URL Filtering on Next Generation Firewall Network Perimeter Device: <ul style="list-style-type: none"> 8.1. Manually convert existing Content Filtering rules to Advance URL Filtering profile. 8.2. Block agreed high risk categories. 8.3. Review with PTA - DOF existing URL Filtering rules and determine necessary parameters for mapping into Next Generation Firewall Networks URL Filtering categories. 8.4. Manually convert an existing URL Content service to NGFW Advance URL Filtering 8.5. Create and implement a Next Generation Firewall Advance URL Filtering policy. 9. Knowledge Transfer Training The winning bidder will provide trainings to PTA technical team on the deployed NGFW. The handover process will covers the installation, configuration, and administration of the NGFW solution. 10. The winning bidder must provide as-built plan documentation. 11. The winning bidder must provide semi-annual Health Check Maintenance with the following as part of a health check service: <ul style="list-style-type: none"> 11.1. Current patch levels. 11.2. Identification of any performance issues. 	
--	--

ml

11.3. Identification of any potential security issues.	
11.4. Identification of any potential server (hardware) issues.	

A. WARRANTY AGAINST BENEFITS

The winning supplier warrants that it has not given nor promised to give any money or gift to any officer or employee of the PTA, or any member of the Bids and Awards Committee, BAC secretariat, or TWG, to secure this contract.

B. ASSIGNMENT

Unless otherwise expressly stipulated or prior written approval of the PTA is secured, this contract or any portion thereof shall not be assigned or subjected to any other party or parties.

I hereby certify that the statement of compliance to the foregoing technical specifications are true and correct, otherwise, if found to be false either during bid evaluation or post-qualification, the same shall give rise to automatic disqualification of our bid.

Name of Company

Signature Over Printed
Name of Authorized
Representative

Date

LOT NO. 2	High Availability (HA) Network Solution, Internet Dedicated Services (IDS) with High Availability, Managed Service - PABX System, Wireless Access Points with Cloud-based Management and Administration and Structured Cabling - Voice and Data
QUANTITY	1 Lot

AGENCY SPECIFICATIONS	BIDDER'S STATEMENT OF COMPLIANCE ²¹
1. INTERNET DEDICATED SERVICE WITH HIGH-AVAILABILITY (IDS-HA)	Brand and Model:
1.1 Two (2) Independent ISP (Primary and Secondary): 150 Mbps each IDS Connection speed with modem/media converter	
1.1.1 Must be a Tier-1 internet provider with multiple submarine cable link support and has fully redundant network routers connected to a high-performance fiber optic infrastructure. <i>"Tier-1 means registered "Telecommunications" Company in the Philippines"</i> The Provider must have a total network traffic capacity of at least 80 Gbps IP upstream (US and Asia)	
1.1.2 The Provider must be ISO 9001:2015 certified, and ISO 27001: 2013 certified.	
1.1.3 The provider must have at least ten (10) years as a telephone and internet service provider from the NTC.	
1.1.4 Must have Seamless Dedicated Internet Premium Bandwidth with High Availability (HA) via fiber connection capable of transmitting multiple traffic streams and variable bandwidth preset with twice the subscribed bandwidth of: Independent Primary ISP = 150 Mbps and Independent Secondary ISP = 150 Mbps.	
1.1.5 Must have an existing Wide Area Network (WAN) fiber-optic backbone near the main entrance of Bangko Sentral ng Pilipinas (BSP) and Department of Finance (DOF) Buildings.	
1.1.6 Must have a Metro-wide fiber optic network	
1.1.7 Must have a Tier I International Internet Exchange backbone connection with the corresponding type of connections (submarine cable, satellite, etc.)	

²¹ Bidders must state here either "Comply" or "Not Comply" against each of the individual parameters of each Specification stating the corresponding performance parameter of the equipment offered. Statements of "Comply" or "Not Comply" must be supported by evidence in a Bidder's Bid and cross-referenced to that evidence. Evidence shall be in the form of manufacturer's un-assembled sales literature, unconditional statements of specification and compliance issued by the manufacturer, samples, independent test data etc., as appropriate. A statement that is not supported by evidence or is subsequently found to be contradicted by the evidence presented will render the Bid under evaluation liable for rejection. A statement either in the Bidder's statement of compliance or the supporting evidence that is found to be false either during Bid evaluation, post-qualification or the execution of the Contract may be regarded as fraudulent and render the Bidder or supplier liable for prosecution subject to the applicable laws and issuances.

1.1.8 Must be able to change traffic with other Tier 1 providers, following strict peering agreements. (Peering is the internet traffic exchange between two networks that have agreed on a connection to exchange traffic without using a third party, reducing internet costs. Without Tier 1 internet providers, internet traffic could not be exchanged between countries.)	
1.1.9 Must be capable of connecting to wan failover and ISP internet load balancing appliance with stable bandwidth connection.	
1.1.10 Must be directly connected from the main pipe of the USA internet backbone and directly connected to the foundations of the internet, offering higher speed connections and more reliable networks.	
1.1.11 Must be connected from the Asia Pacific loop of a backbone with the East-Asia Crossing and Pacific Crossing.	
1.1.12 Must be a member of a Local Internet Exchange, e.g., Philippine Internet Exchange (PhiX), Matrix Internet Exchange (MIX), Common Routing Exchange (CORE), etc.	
1.1.13 Must guarantee a 1:1 ratio of bandwidth from the user's office to the global Internet	
1.1.14 Must have a flatter network optimized for IP with low latency	
1.1.15 Must be capable of a redundant node from PTA Site to the ISP's main hub.	
1.1.16 Must perform a Bit Error Ratio (BER) Testing after installation.	
1.1.17 Must Supply a Committed Information Rate (CIR): No less than 150Mbps each independent ISPs.	
1.1.18 Must provide Public IP addresses (PIP): IP allocation should be flexible and easier to access from a Tier 1 provider. a. /30 and /27 for the ISP1, and b. /30 and /27 for the ISP2	
1.1.19 The facility Must be owned and operated by the Internet Service Providers (ISPs).	
1.1.20 Must perform Local Area Network (LAN) and Wide Area Network (WAN) equipment configurations.	
1.2 TWO (2) UNITS MANAGED SERVICE TELCO GRADE ROUTER FOR EACH INDEPENDENT ISP: Cisco ISR 4351 routers including subscriptions and Local supports with the following specifications:	
1.2.1 Form Factor: 1ru	

1.2.2 Performance: 500 Mbps throughput upgradable to 2Gbps	
1.2.3 Management Port with Management Cable	
1.2.4 Network Interface Module (NIM): 3	
1.2.5 Default / Max Dram: 8 GB / 16 GB	
1.2.6 Integrated Services Card Slots: 1 (PVDM 4)	
1.2.7 USB ports (type A): 2	
1.2.8 Power Supply Type: Internal AC, POE, or DC	
1.2.9 Redundant Power Supply:	
1.2.10 Module online insertion and removal	
1.2.11 Server virtualization platform (UCS E Series) and Network Compute Engine (NCE): 4 Core NCE	
1.2.12 Zone-based firewall and NAT services:	
1.2.13 VRF- aware Firewall and Network address translation (NAT)	
1.2.14 Hardware VPN acceleration (DES, 3DES, AES)	
1.2.15 IPSEC VPN Services:	
1.2.16 Flex VPN, Easy VPN remote server, Enhanced Easy VPN, Dynamic Multipoint VPN (DMVPN)	
1.2.17 Group encrypted transport VPN (GET VPN), V3PN, MPLS VPN	
1.2.18 Intrusion Prevention: Snort for signature Based and Firepower as nGIPS	
1.2.19 Anomaly Detection and Machine Learning: Cisco Self Learning Networks (SLN)	
1.2.20 Network Foundation Protection: ACL, FPM, control plane protection, control plane policing (capp), Qos role-based CLI access, source based RTBH, uRPF, SSH v2	
1.2.21 Cisco Umbrella Branch Support	
1.2.22 Cisco Cloud web security <ul style="list-style-type: none"> a. Cisco trust Sec b. Security Group tag Exchange Protocol (SXP), SGT over GETVPN 	
1.2.23 SGT over IPSEC	
1.2.24 SGT over DMVPN	
1.2.25 SGT-based ZBFW	
1.2.26 Port/Layer 3 interface/IP/Subnet-to-SGT mapping	
1.2.27 SGT export in Flexible Netflow	
1.3 ONE (1) UNIT LOAD BALANCER INTERNET ACCESS GATEWAY APPLIANCE.	

<p>1.3.1 Hardware & Performance Profile:</p> <p>a. The proposed solution must be a 1RU appliance</p> <p>b. The proposed solution must meet the performance specification below:</p> <p>c. Firewall throughput 12Gbps.</p> <p>d. New connections(TCP)80,000.</p> <p>e. Threat prevention throughput 4.2Gbps</p> <p>f. IPS Throughput 3.85 Gbps</p> <p>g. The proposed solution must provide the type & number of interfaces as below:</p> <ul style="list-style-type: none"> • At least two (2) USB ports • At least six (6)10/100/1000 Base-T ports • At least 2 SFP ports • At least two (2) 10G ports with end to end SFP Modules. <p>h. Hard Disk - The proposed solution must provide 64Gb SSD disks</p>	
<p>1.3.2 Network Adaptability</p> <p>a. Deployment</p> <p>b. The product proposed should support following deployment modes:</p> <ul style="list-style-type: none"> • routing/gateway mode; • transparent/bridge mode • virtual wire mode • bypass mode. • Mixed mode 	
<p>1.3.3 Hardware Bypass</p> <p>The product proposed must support at least 2 pair of hardware bypass(copper), so in case of device failure, the network traffic can still pass.</p>	
<p>1.3.4 High Availability</p> <p>The proposed product must support high availability via.</p> <ul style="list-style-type: none"> • Active-Active mode; • Active-Passive or Active Standby mode; 	
<p>1.3.5 Link Aggregation</p> <p>The proposed product must support link aggregation with following work mode:</p> <ul style="list-style-type: none"> • Load balancing - hash • Load balancing - RR(Round Robin) • Active-Passive • LACP 	
<p>1.3.6 Link State Propagation</p> <p>The proposed product must support link state propagation, that means can setup the correlation interface group, if one of the interface in the group</p>	

turns up/down, the other interface will follow the same action	
1.3.7 Link State Detection The proposed product must support link state detection, with at least the methods below: <ul style="list-style-type: none"> • Address Resolution Protocol (ARP) • Packet Internet or Inter-Network Groper (Ping) or ICMP • Domain Name Server (DNS) Lookup 	
1.3.8 Network Address Translation (NAT) The product proposed must support different mode of NAT: <ul style="list-style-type: none"> • SNAT, DNAT and bidirectional NAT. • One to one NAT, one to many, many to one NAT. • NAT46, NAT64 	
1.3.9 IPv6 The product should be ready for IPv6, include: <ul style="list-style-type: none"> • Support IPv4/IPv6 dual stack mode; • Support control IPv6 in access control policy, provide control via IP address, service, application, domain.etc. 	
1.3.10 Dynamic Host Configuration Protocol (DHCP) The product should support DHCP, include: <ul style="list-style-type: none"> • Act as DHCP server or DHCP proxy • Support IP reservation 	
1.3.11 Generic Routing Encapsulation (GRE) The product proposed should support GRE tunnel.	
1.3.12 Others <ul style="list-style-type: none"> • Support DNS transparent proxy • Support ARP proxy • Support DDNS 	
1.3.13 Routing Static Route The product proposed must support static routing.	
1.3.14 Dynamic Routing The product proposed must support dynamic routing protocol: <ul style="list-style-type: none"> • Routing Information Protocol (RIP)v1/2 • Open Shortest Path First (OSPF)v2, OSPFv3 • Boarder Gateway Protocol (BGP)4 	
1.3.15 Open Shortest Path First (OSPF) Support redistributes direct route, static route, RIP route (OSPFv2), default route to OSPF. Support authentication method: plaintext, MD5	

<p>1.3.16 Boarder Gateway Protocol (BGP) Support redistribute direct route, static route, RIP route, OSPF route to BGP</p>	
<p>1.3.17 Policy-Based Route: The product proposed must support policy-based route. The policy route can setup with:</p> <ul style="list-style-type: none"> • Routing source can be specific to IP, IP group • Support select route based on IP, services, Country/Region, Application etc. • Support load balance via at least 4 methods, Round Robin, Bandwidth ratio Round robin, Weighted least traffic, prefer the first link (link on top) 	
<p>1.3.18 IPsec Virtual Private Network (VPN) The proposed product must support at two types of IPsec VPN protocols:</p> <ul style="list-style-type: none"> • Proprietary VPN protocol. • Standard IPsec protocol. 	
<p>1.3.19 Dynamic Connection The product proposed must be able to setup site to site VPN in the following scenarios:</p> <ul style="list-style-type: none"> • Both site is static IP • Both site is dynamic IP • One site is dynamic IP while the other site is static IP 	
<p>1.3.20 VPN Status Monitoring Support monitoring the status of each VPN tunnel, the data be monitoring includes:</p> <ul style="list-style-type: none"> • Overview of all the active VPN tunnels • Inbound/outbound traffic; • Latency • Packet loss rate; 	
<p>1.3.21 Software Defined-Wide Area Network (SD-WAN) The solution proposed should support SD-WAN capability via VPN tunnels:</p> <ul style="list-style-type: none"> • Support session-based link balancing mode. • Can choose the optimize link based on bandwidth-remaining ratio, application type or link quality (means packet loss, jitter, latency) 	
<p>1.3.22 Others a.Support IPsec VPN as the backup link, when main link (MPLS or lease line) disconnected, the traffic will failover to IPsec tunnel b.Support Access Control, Security policy (IPS, APT etc) on IPsec tunnel.</p>	
<p>1.3.23 Secure Socket Layer (SSL) VPN</p>	

<p>The proposed product should support SSL VPN feature.</p> <ul style="list-style-type: none"> • Support at least 30 concurrent user access • Support TCP, UDP, ICMP protocols • Support HTTP, HTTPS, Email, Fileshare, FTP etc. • Support control access by IP, URL, TCP/UDP port etc. • Support access resource (destination IP/system) by NAT (NGAF IP address) or virtual IP 	
<p>1.3.24 Operating System and Browser The proposed product should be able to support SSL VPN access via Windows XP/7/8/10, MacOS, Andriod, IOS</p>	
<p>1.3.25 Active Directory Support</p> <ul style="list-style-type: none"> • Support LDAP user automatic synchronization. • Support Microsoft AD security group mapping. • Support SSL VPN user log in & log out log 	
<p>1.3.26 User Authentication The proposed product should be able to support user authentication via following standard:</p> <ul style="list-style-type: none"> • Support captive-portal based authentication; the captive portal is customizable; • Support Single Sign-on (SSO) with Microsoft AD, Radius • Support local user database, and external user authentication such as LDAP, Radius, POP3 etc. 	
<p>1.3.27 Access Control The proposed solution should support application control feature and meet the following specifications:</p> <ul style="list-style-type: none"> • Support application control and can identify & control over 9800+ applications. • Support admin customize their own application types • Typical types of applications can be controlled include game, P2P, shopping, social networking etc. • Should be able to control applications via source/destination IP, username, Schedule etc. • Be able to deny, allow applications 	
<p>1.3.28 Uniform Resource Locator (URL) Filtering</p>	

<p>The proposed product must support URL filtering:</p> <ul style="list-style-type: none"> • provide at least 70+ URL categories, include game, gambling, finance, Pornography etc. • Support manually create customized the URL category. • Should provide on premise URL signature database, not only rely on cloud. 	
<p>1.3.29 File Filtering The proposed solution must support filter, which can filter the download, upload file by file type(extension).</p> <ul style="list-style-type: none"> • Support common file type(extension) category, such as, image, text, executable file, scripts etc. • Support customized file type(extension) 	
<p>1.3.30 Connection Control The proposed solution should support feature to control concurrent session/connections:</p> <ul style="list-style-type: none"> • Be able to control concurrent session/connect by source IP, destination IP, or both • In the policy, it will be able to setup specific concurrent session/connection number. 	
<p>1.3.31 Geolocation Control The proposed product should be able to control traffic based on Geolocations:</p> <ul style="list-style-type: none"> • Be able to control the source IP by a geolocation level, that means the device have a database that can identify the access (IP) is from which country/region and specify the deny or allow action • The geolocation identifications should be able to support to the major countries in the world • Support the search feature to help find out a specific IP belong to which region. • Support check the status of IP that being blocked. • Support exclude specific IP from the control. 	
<p>1.3.32 Bandwidth Management The product proposed must be able to support bandwidth management feature:</p> <ul style="list-style-type: none"> • Be able to limit or guarantee the bandwidth based on IP, user, application, schedule, VLAN etc. 	

rd

<ul style="list-style-type: none"> • Be able to provide per IP/User speed control in single policy 	
<p>1.3.33 Security Protection Overall Intrusion Prevention System (IPS) The product propose must support IPS feature and meet the specification below:</p> <ul style="list-style-type: none"> • IPS signature over 9000 entries on premise. • Support admin create customized IPS signature by regular expression, keywords, protocol, port & direction • Support admin change the signature default action by per signature based or global. • User can use CVEID, Vulnerability Name, vulnerability ID, threat level etc to search for the related signature. • IPS module should be able to detect brute-force attack to DB2, Mongoddb, MSSQL, MySQL, FTP, IMAP, Jboss, Jenkins, Joomla, Kerberos, SMB, Telnet, SSH, RDP etc. • IPS can get up to date signature data via cloud threat intelligence or upload signature package via web UI • Support minimize to 10-minute update after a new outbreak happens, when connect to cloud threat intelligence 	
<p>1.3.34 Advance Persistent Threat (APT) Support Feature</p> <ul style="list-style-type: none"> • The proposed solution must support APT and meet the following: • Detection of remote control trojan, malicious URL/domain, and other threats. • The product should support at least 140 million malware signature database on premise • The device can connect to cloud threat intelligence and do real-time for check to threat that cannot be identified locally. • APT can effectively identify & block the abnormal traffic within well-known protocols such RDP, SSL, IMAP, SMTP, POP3, FTP, DNS, HTTP, WEB 	
<p>1.3.35 Anti-Virus Support Feature The proposed solution must support anti-virus feature:</p> <ul style="list-style-type: none"> • Support stream based anti-virus with AI-Based anti-virus engine • Support protocols HTTP, HTTPS, FTP, SMTP, IMAP, POP3, SMB etc. 	

nd

<ul style="list-style-type: none"> • Support compress file detection, and support compress file with up to 16 layers. • Support scan the files up to 20MB • Support detect virus in main stream file types, include text, image, music, movie, compressed file, executable file, document, script,etc. • Support cloud based analysis with the file cannot be identified locally • Support whitelist or exclude trusted file by MD5 or URL path 	
<p>1.3.36 Anti-DoS/DDoS (Denial of Service) The proposed solution must support anti-dos/ddos features, with the features:</p> <ul style="list-style-type: none"> • Support ARP flood, SYN flood, UDP flood, DNS flood, ICMP&ICMPv6 flood protection. • Support IP/port scan protection. • Support detection and prevent Tear Drop attack, LAND attack, Win Nuke attack, Smurf attack, Ping of death, IP fragment. 	
<p>1.3.37 Cloud Threat Intelligence The proposed solution should provide the cloud-base threat intelligence capabilities, include:</p> <ul style="list-style-type: none"> • Cloud Sandboxing • Cloud intelligence to identify unknown/new threats • Cloud intelligence can provide the new signature update to new outbreaks, the minimized respond time is 10 minutes. 	
<p>1.3.38 Decryption The proposed solution must support HTTPS decryption</p>	
<p>1.3.39 Account Protection The proposed solution must support a dedicated account protection module to identify the abnormal usage of user accounts.</p> <ul style="list-style-type: none"> • Support detection of weak password, brute-force attack, abnormal/suspicious login etc. • Provide dedicated GUI page to show & respond all the account abnormal usage events that happens recently. 	
<p>1.3.40 Ransomware Protection The proposed solution must support a dedicated ransomware protection module, which can:</p>	

<ul style="list-style-type: none"> • Automatically scan and detect ransomware related vulnerabilities, port, weak password, brute-force attack etc. • Provide dedicated GUI page to show and respond all the ransomware related vulnerabilities • Can provide guidance or suggested action to admin, e.g., deploy block policy direct, 	
<p>1.3.41 Security Assessment Risk Analytics</p> <p>a.The proposed solution must provide risk analytics module that allows to scan and identify security loopholes such as open port, system vulnerabilities, weak passwords, etc.</p> <p>b.The risk assessment should support major protocols such as: HTTP, HTTPS, POP3, SMTP, RDP, SMB, Oracle, MS-SQL, MySQL etc.</p>	
<p>1.3.42 Passive Vulnerability Scan</p> <p>a.The proposed solution must provide a real-time vulnerability analysis or passive vulnerability scan:</p> <ul style="list-style-type: none"> • Detection vulnerabilities based on traffic pass through NGAF, without any active scanning activities to the servers, minimize the extra work load and other impact • The vulnerabilities that can be detected includes web application vulnerability, weak password, improper configuration on web server, etc. • Support generate HTML format report 	
<p>1.3.43 Log and Reporting</p> <p>a.The proposed solution must support build-in log center which can keeps 4 types logs:</p> <ul style="list-style-type: none"> • Access Log (Application control log, user authentication log, SSL VPN log) • Security Log (IPS, WAF, Botnet, Email protection, Anti DoS, Web Access) • System log • Support export log to excel file. <p>b.The appliance should include the local hard disk to provide log retention</p>	
<p>1.3.44 Reporting</p> <p>The proposed solution must support build-in reporting features, which include:</p> <ul style="list-style-type: none"> • Generate comprehensive Security report in PDF format • Support security report subscription by email, in daily, weekly, monthly based. 	

1.3.45 Syslog The proposed solution must support export log to syslog server	
1.3.46 Certifications - CyberRatings The proposed solution must be with "AAA" racking in the Cyber Ratings Enterprise Firewall	
1.3.47 Capability Maturity Model Integration (CMMI) Vendor must be certified with CMMI L5.	
2. MANAGED SERVICE - PABX SYSTEM	
2.1 PABX System must have minimum capacity of the following configuration:	
<ul style="list-style-type: none"> 2.1.1. One (1) ISDN Port Thirty (30) Channels 2.1.2. Ten (10) Vocoder Channels for SIP Trunks 2.1.3. 10 SIP Ports 2.1.4. 25 IP Subscriber Licenses 2.1.5. One (1) Operator IP Phone 2.1.6. Twenty-Four (24) Enterprise IP Phones 	
2.2 Operator IP phone must be paired with DSS expansion key	
2.3 The IP-PBX/PABX/Communication System shall employ IP at its core with IP switching technology and 100% non-blocking.	
2.4 The system should be IPV6 ready.	
2.5 The architecture of the system shall be capable of seamless migration to its maximum capacity by simply adding peripherals cards/modules in the same chassis without compromising function/features of the system. The architecture should be non-stackable eliminating individual power supply for each chassis.	
2.6 The system should be built on a universal slot architecture and modular in design to enable seamless growth, by adding the desired necessary modules and cards as and when required. Any interface peripheral card can be inserted in any slot of the platform, whereby it is possible to increase or decrease the trunk lines or subscriber lines of the system as per the requirement.	
2.7 It shall have distributed processing architecture, SLIC and SMT Design.	
2.8 The system shall have the built-in Auto-attendant facility and shall be able to answer minimum 9 calls simultaneously and should support dial-by-name.	
2.9 The system shall be compatible and type-approved with ISDN PRI line of Local Service Provider.	
2.10 The PRI card should be software programmable for TE/NT mode.	

2.11 Two (2) units 24 ports Power Over Ethernet (POE) Switch must be included to provide power to the IP phones	
2.12 The system shall have built-in web-based software programming tool for system administration.	
2.13 Detail reports of all system parameters should be generated through the SMDR port of system.	
2.14 Each port of the system shall be programmable. It shall have programmable features port-wise/extension-wise.	
2.15 The system shall support flexible numbering for extensions such as it may have extensions with 1 digit, 2 digits and up to 6 digits' numbers as well as in combination of all.	
2.16 Access codes, system timers and access to features shall be programmable.	
2.17 Storage of outgoing, incoming and internal call reports shall be generated on SMDR port of the system. It shall also be available online through Ethernet Port.	
2.18 System must have a built-in station message detail recording to log calls without any added modules	
2.19 Provision of PABX telephone system must include the installation, configuration and after-sales service support	
2.20 Full Comprehensive Warranty (12 Months) for PABX system and telephone handsets	
2.21 Knowledge Transfer and End-User Training must be provided after commissioning	
2.22 1x Fiber I LEC 10MB - for remote extension within the building up (comes with Wi-Fi Router (4 Port), /29 IP Block, 1GB of either email or web Hosting Service and MRTG Access	
3. NETWORK EQUIPMENT	
3.1. Core Switch 3.1.1. Managed switch with 12 x 10G copper ports + 12 x 10G SFP+ modules (dedicated) 3.1.2. 1 Gigabit Ethernet Management port 3.1.3. 1RU Height Rackmount 3.1.4. 480Gbps switching capacity 3.1.5. With MTBF of around 1,372M (hours) at 25°C 3.1.6. 3MB Packet Buffer 3.1.7. 240mpps (64-byte packets) 3.2. 24-Port PoE Gigabit Switch 3.2.1. Equipped with 24 Gigabit Ethernet Ports Full PoE+ x 4 10 Gigabit Ethernet 3.2.2. Supports PoE budget of 370W on full load on a single power supply 3.2.3. Max power consumption < 440W on full load	

<ul style="list-style-type: none"> 3.2.4. Supports up to 128 Gbps switching capacity 3.2.5. With MTBF of around 698K (hours) 3.2.6. Rack mountable 	
<ul style="list-style-type: none"> 3.3. 48-Port Gigabit Switch <ul style="list-style-type: none"> 3.3.1. Equipped with 48 Gigabit Ethernet + 4 10 Gigabit Ethernet ports 3.3.2. Supports 176 Gbps switching capacity 3.3.3. Supports up to 8K MAC addresses 3.3.4. With MTB of around 1.452M (hours) 3.3.5. Rack mountable 	
<ul style="list-style-type: none"> 3.4. Indoor Wi-Fi 6 Access Points <ul style="list-style-type: none"> 3.4.1. Cloud managed Access Point with integrated enterprise security and guest access 3.4.2. 2x2:2 (2.4GHz) + 4x4:4 (5GHz) MU-MIMO 802.11ax 3.4.3. Application-aware traffic shaping 3.4.4. Enhanced transmit power and receive sensitivity 3.4.5. Supports automatic cloud-based RF optimization 3.4.6. With MTB of around 500K (hours) 	
<ul style="list-style-type: none"> 3.5. Network Monitoring Software <ul style="list-style-type: none"> 3.5.1. Supports 4 monitoring engine to provide users with efficient, scalable monitoring 3.5.2. With dashboard that provides a customizable high-level overview of hosts, services, and network devices 3.5.3. Can easily view network incidents and resolve them before they become major catastrophes 3.5.4. Automated, integrated trending and capacity planning graphs allow organizations to plan for upgrades 3.5.5. Equipped with configuration wizards & infrastructure management 3.5.6. Supports advanced user management to easily setup and manage user accounts with only a few clicks then assign custom roles to ensure a secure environment 	
<p>4. STRUCTURED CABLING Supply, delivery and installation of network peripherals and cabling materials for 100 nodes</p>	
<ul style="list-style-type: none"> 4.1 Cat6 UTP Cable <ul style="list-style-type: none"> 4.1.1. 10/100/1000 BASE-TX 4.1.2. Bare Copper Material, 23 AWG Construction Conductor 	

<p>4.1.3. HDPE Material Insulation 4.1.4. PE Cross Member 4.1.5. ISO/IEC 11801 ED.2.2:2011 Compliant 4.1.6. ANSI/TIA 568-c.2-2011 Compliant</p>							
<p>4.2. Cat6 Patch Panel 4.2.1. IDC connector can accept 22-26 AWG solid and stranded cables. 4.2.2. Terminate using 110 or Krone Tools 4.2.3. Dimensions and mounting compliant with EIA-310-D 4.2.4. Panel Area: SECC/1.5mm thickness 4.2.5. Number of ports/ height: 24/1U 4.2.6. Color: Black 4.2.7. Easy port description by removable labels in plastic holders. 4.2.8. RoHS Compliant</p>							
<p>4.3. CAT6 Modular Plug / RJ45 Connector - Unshielded 4.3.1. UL Applications that support up to 250V AC 4.3.2. Dielectric with standing voltage 500V AC 4.3.3. 100Mohms Insulation Resistance 4.3.4. Transparent Polycarbonate 4.3.5. Phosphor bronze blade w/ gold plating</p>							
<p>4.4. UTP Cable Management Guide 1U 4.4.1. 19" Standard rack and cabinet mountable 4.4.2. Meets EIA/TIA bend radius requirements. 4.4.3. Prevents cable tangles 4.4.4. Light weight and easy to install. 4.4.5. The panel is configured with 12 rings. 4.4.6. Two (2) openings in the rear to provide access pathway 4.4.7. ROHS Compliant</p>							
<p>4.5. Cat6 UTP Patch Cord 4.5.1. Category 6 UTP patch cord using RJ45 contacts 50u inch gold plated and snag proof boot. 4.5.2. 10/100/1000 BASE-T, Voice, Video and other applications</p>							
<table border="1"> <tr> <td data-bbox="203 1759 386 1822">Conductor</td> <td data-bbox="386 1759 521 1822">Material / Size</td> <td data-bbox="521 1759 906 1822">Bare Copper / 30 AWG</td> </tr> <tr> <td data-bbox="203 1822 386 1894">Insulation</td> <td data-bbox="386 1822 521 1894">Material</td> <td data-bbox="521 1822 906 1894">High Density Poly Ethylene (HDPE)</td> </tr> </table>	Conductor	Material / Size	Bare Copper / 30 AWG	Insulation	Material	High Density Poly Ethylene (HDPE)	
Conductor	Material / Size	Bare Copper / 30 AWG					
Insulation	Material	High Density Poly Ethylene (HDPE)					



	Diameter	0.55 ± 0.05 mm	
Sheath	Material	Low Smoke Zero Halogen (LSOH)	
	Diameter	3.1 ± 0.2 mm	
4.6 19" Open Bay Rack, Floor Mount			
4.7 One (1) unit UPS Rack mountable/tower, 2000VA 230V- 1800 Watts or higher			
<p><u>SCOPE OF WORK -</u></p> <p>The Winning Bidder shall provide the service to the Philippine Tax Academy (PTA) in accordance with the terms and conditions and must include the following provision of service:</p> <ol style="list-style-type: none"> 1. Must provide Design and Planning of the service to be provided. 2. The Winning Bidder must Supply, Deliver, Configure, and Install: <ol style="list-style-type: none"> 2.1. Two (2) Independent Internet Service Providers (ISPs) with One Hundred Fifty (150) Mbps Committed Information Rate (CIR) each via Fiber Optic Cable to the PTA Office located at 3rd floor, DOF Main Building and 7th floor, EDPC Building, BSP Complex Roxas Blvd., cor. P. Ocampo St., Manila. 2.2. Two (2) units Managed Service Telco Grade Router for each independent ISP: Cisco ISR 4351 routers including subscriptions and Local supports. 2.3. One (1) unit Managed Service Load Balancer Internet Access Gateway appliance. 2.4. Managed service PABX System 2.5. One Hundred (100) nodes of structured cabling 3. Installation cost must be bundled with the one-year contract service, including providing the needed cables/insulation and other related materials following industry standards. 4. Suppose the PTA transfers to a new office location. In that case, the Provider must transfer the Fiber Optic Cable (FOC) connection, including hardware re-deployment, to the new site at no cost. 5. Must conduct Acceptance testing, which will be used as the basis for the start of the billing period for the internet service (ISP); shall take 			

place after the installation and inspection, subject to the following criteria:

- 5.1. Must be conducted by the winning Internet Service Provider /Telecommunications Company (ISP/Telco) in the presence of PTA-ITD representatives;
- 5.2. No service interruption must take place during the testing period, except for those beyond the provider's control (i.e., power failure, failure of equipment, and international/regional backbone problems);
- 5.3. Committed Information Rate (CIR) requirement compliance for two (2) proposed independent ISPs;
- 5.4. Latency requirement compliance;
- 5.5. Must turn over an assigned Multi-Router Traffic Grapher (MRTG) accounts for both independent ISPs to PTA-ITD;
- 5.6. Must secure and provide usable static public IP-Address as required.
- 5.7. Must conduct Bit Error Rate (BER) Test.
- 5.8. The Acceptance Test Procedure must have the following results:
 - 5.8.1. Line Quality Test - Test: BER - Standard: **Error – free**
 - 5.8.2. Test for Packet Loss - Test: Ping - Standard: **100% packet return**
 - 5.8.3. Latency Test - Ping - Standard: **180-250 milliseconds to US routes.**
6. **Technical Support:** Technical support services must include the following:
 - 6.1. Maintenance Services
 - 6.1.1. Maintenance of all provided hardware, peripherals, and Software to ensure proper working order;
 - 6.1.2. Replacement of all defective hardware peripherals and materials in case of hardware malfunction;
 - 6.1.3. Pro-active notification thru email, phone calls, and SMS on any occurrences of the following:
 - a. Schedule downtime
 - b. Service interruption
 - c. Upgrades or preventive maintenance

- d. Possible rerouting of internet connection to backup link due to connection loss of both primary and secondary links.

6.2. Customer support

- 6.2.1. 24x7 on-call support;
- 6.2.2. Must resolve all kinds of technical problems within 30 minutes from the initial report time, including but not limited to:
 - a. When the links connection is down
 - b. Packet loss
 - c. Latency variation
 - d. Routing issue
- 6.2.3. Must provide an hourly status update from receipt of initial report time if trouble will take more than 30 minutes to resolve;
- 6.2.4. Must provide telephone (landline/cellphone), SMS, or Email technical support, available on a 24x7 basis to assist in troubleshooting issues;
- 6.2.5. Must provide qualified technical representative/s, within 24 hours of initial report time and at no additional cost to PTA, for issues that need to be resolved on-site.

6.3. Service Level Agreement

- 6.3.1. Must provide Network Availability of: 99.8%
- 6.3.2. Must have 24/7 network support and data operations center
- 6.3.3. Must have an Upgradeable and Scalable Bandwidth Provisioning
- 6.3.4. Must have a robust and resilient network
- 6.3.5. Must have an extensive nationwide network
- 6.3.6. Must have experienced and licensed technical support engineers for the required managed routers and equipment, preferably Cisco Certified Network Associate

<p>(CCNA) and Cisco Certified Network Professional (CCNP)</p> <p>6.3.7. Must provide guaranteed latency not less than 200ms at 50% load from PTA to the internet service provider</p> <p>6.3.8. Must have a guaranteed Packet Loss of 0.1% or less</p> <p>6.3.9. Provide PTA a written notice at least (5) working days before the scheduled maintenance work. In the event of service interruption due to scheduled maintenance, the provider should have alternate re-routing of the internet connection.</p> <p>6.3.10. Mean-Time-To-Repair (MTTR)</p> <p>6.3.11. Router Connection Error (30-45 mins)</p> <p>6.3.12. Local Exchange Breakdown (2-4 hrs)</p> <p>6.3.13. Scheduled Maintenance Work (4-6 hrs)</p> <p>6.3.14. Must provide a monthly report of service interruption and time of delay with corresponding rebates, if there are any.</p> <p>6.3.15. Diverse and distributed cable routes using trans-Asia and trans-Pacific submarine cable systems with redundancy</p> <p>6.3.16. Must provide a direct connection to major IXs (Internet Exchanges), both local and international</p> <p>6.3.17. Minimum of 1:1 Committed Information Rate (CIR) synchronous download and upload.</p> <p>6.3.18. Must provide real-time access to bandwidth utilization monitoring reports through Multi Router Traffic Grapher (MRTG) for two (2) circuits.</p>	
<p><u>DELIVERY AND RECEIVING INSTRUCTIONS</u></p> <p>The Supplier shall observe the following instructions:</p>	

16

<ol style="list-style-type: none"> 1. Services/Goods as specified in this Schedule of Requirements and/or the Technical Specifications must be delivered only to the address indicated herein. 2. The Provider must notify the indicated authorized receiving personnel at the Project Site of the scheduled delivery date at least three (3) working days in advance and shall ensure that the authorized receiving personnel from the PTA is present during the date and time of delivery. 3. The Supplier shall deliver to the Project Site from 9:00 AM to 6:00 PM and on Mondays to Fridays only; the Provider shall not make deliveries before 9:00 AM, after 6:00 PM, and on non-working days. 4. Upon delivery of the Goods to the Project Site, the supplier shall notify the PTA and present the following documents: <ol style="list-style-type: none"> 4.1. Original Supplier's Invoice showing the Goods description, quantity, unit price, and total price. 4.2. Original Delivery Receipts 4.3. Original Statement of Accounts. 4.4. Approved Purchase Order for these conditions, Purchaser's representative at the Project Site is Mr. Mark P. Olaguir, Development Management Officer III, and concurrent Technical Property Inspector or his authorized representative(s). 	
<p><u>WARRANTY AND MAINTENANCE:</u></p> <ol style="list-style-type: none"> 1. Six (6) months workmanship warranty for structured cabling 2. One (1) year warranty for ICT equipment such as APs, routers, switches, and racks. 3. With parts and on-site service support for all equipment during the whole duration of the warranty. 4. After-sales support services with committed Service Level Agreement of 99.8%. Customer Service Center facilitates communication between customers and various technical levels within 24 hours x 7 days a week basis. 	
<p><u>DOCUMENTARY REQUIREMENTS:</u></p> <ol style="list-style-type: none"> 1. Duly Notarized Declaration of the following: <ol style="list-style-type: none"> 1.1. Must have Fiber Optic Cable Multiplexer and Gigabit Ethernet (GE) capable, Interface Hand-off: (Gigabit Ethernet 10/100/1000 - electrical) 	

no

<ul style="list-style-type: none"> 1.2. Must have at Least 1Gbps Multi-Lateral Peering with Phopenix for at least six (6) years. 1.3. Must have at least ten direct International Uplinks (Tier 1/Tier 2, ie. AT&T, Level 3, Telstra, etc.) for redundancy purposes. 1.4. Minimum total Uplink capacity of 40Gbps to 130Gbps 1.5. Managed and operated local Internet peering (i.e., MIX, GIX, PHIX) 1.6. High Speed and Dedicated Internet service with 1:1 CIR (Committed Information Rate) <p>2. Must Provide a Detailed Diagram of the Following:</p> <ul style="list-style-type: none"> 2.1. at least 10 direct International Uplinks (Tier 1/Tier 2, ie. AT&T, Level 3, Telstra etc.) for redundancy purposes. 2.2. Backhaul going to Cable Landing Station (i.e Nasugbu, Batangas, Naic Cavite) 	
<p><u>QUALIFICATIONS OF THE SERVICE PROVIDER</u></p> <p><u>The Contractor should have the necessary eligibility, experience, and expertise in providing service the following:</u></p> <p>A. Eligibility Requirements:</p> <ul style="list-style-type: none"> 1. PhilGEPS Platinum Membership Registration Certificate/Number; 2. Mayor's/Business Permit (current and valid); 3. Tax Clearance; 4. Omnibus Sworn Statement (duly notarized); and 5. Other mandatory documents are required in Competitive Bidding under Implementing Rules and Regulations of RA No. 9184 <p>B. Expertise Requirements</p> <ul style="list-style-type: none"> 1. At least five (5) years of experience providing Wireless Network Solutions. 2. At least ten (10) years as telephone 	

e

service provider and at least ten (10) years as Internet Service Provider.

3. Must submit a Letter from the Principal Certifying Partnership, Experience, and Capability.

The contractor who has completed, within the last five (5) years from the submission and receipt of bids, a single largest contract similar to the Contract to be bid.

The prospective bidder shall also be required to include in this proposal original descriptive kinds of literature and unamended brochures of all equipment/materials to be supplied. If applicable, plans, drawings, and diagrams/configurations must likewise be provided.

THE FOLLOWING ARE ADDITIONAL REQUIREMENTS WHICH WILL BE PART OF THE TECHNICAL BID DOCUMENTS:

1. All prospective bidders shall have a track record of existing installations of the offered network equipment's and structured cabling system in the Philippines.
2. The following certifications must be provided:
 - a. All prospective bidders must be authorized dealer of all equipment to be supported by certificate of dealership in the Philippines issued by the manufacturer/distributor of equipment/materials.
 - b. All prospective bidders must be capable of rendering local technical services duly certified by the manufacturer/distributor.
 - c. The bidder must have at least Three (3) Certified Licensed Electronics Engineers who are currently employed in the bidder's company trained and certified in the design and installation of Access Points. Bidder must attach certification.

- d. Must provide 2 CCNA, 2 CCNP, 2 CCIE, and must be employed in the company.
 - e. The Bidder must be an ISO 9001:2015 and ISO 27001:2013 certified company.
 - f. The bidder provider must secure an NTC certification that they are a Tier1 Telco Company.
 - g. The bidder shall have a Fiber Optic Cable Multiplexer and shall be Gigabit Ethernet (GE) capable. Interface Hand-off: (Gigabit Ethernet 10/100/1000 - electrical)
 - h. Must have at Least 1Gbps Multilateral Peering with PHOpenIX for at least six (6) Years and shall Provide certification.
3. Network Requirement:
 - a. Must have at least 10 direct International Uplinks (Tier 1/Tier 2, ie. AT&T, Level 3, Telstra etc.) for redundancy purposes. Bidder shall provide detailed diagram.
 - b. Must have/operate its own Backhaul going to Cable Landing Station (i.e Nasugbu, Batangas and Naic, Cavite). Bidder shall provide detailed diagram.
 - c. Provider must have a minimum total Uplink capacity of 40Gbps (to address needs of client/s) and must provide proof therein.
 - d. Manage and operate local Internet peering (i.e. MIX, GIX, PHIX) and provide certification therein.
 4. Shall submit Certificate of Employment of at least two (2) Information Technology Infrastructure Library (ITIL) Certified Engineers and shall provide proof of certification for ITIL.
 5. Shall submit network layout labeled as Electronics Engineer Plan showing connectivity from end user's data terminal facility up to the last mile duly signed by Licensed Electronics Engineer (EE) with his/her valid PRC ID.
 6. Should submit copies of Client Satisfactory Certificates from at least

<p>three (3) clients each for the last three (3) years for similar contracts.</p> <ol style="list-style-type: none"> 7. Must be an NTC registered and certified with Value Added Services (VAS) Registration license certificate. 8. Bidders should be a certified Data Center Provider/Back up provider Tier III. Bidder shall provide proof. 9. All prospective bidders may request the conduct a site survey and submit a report regarding the site survey. 10. All prospective bidders shall submit their proposed Service Level Agreement (SLA) and commits to deliver and maintain their service with a Service Level Agreement of 99.8%, as stated above under the Scope of Work and provide Customer Service Center which facilitates communication between customers and various technical levels within <i>24 hours x 7 days a week basis</i>. 11. All prospective bidders shall submit original copy of design proposal, brochures and other publications that supports compliance to the requirements. 12. Provide and submit a proposed work plan and detailed implementation Schedule /Gantt Chart for the Project covering the whole contract period. Prospective Bidders are required to conduct site inspection. This is to ensure the reliability, security and efficiency of the required services that the contractor shall perform. Timeframe should be specified or each activity to be done and shall include Gantt Chart Summary. 	
<p><u>TRAINING REQUIREMENTS</u></p> <p>Prior to Final Acceptance, the supplier shall provide End-user training on how to use and manage the active components included in the project.</p> <p>The winning bidder shall also provide the end-user with user, configuration and technical manuals.</p>	

BILL OF MATERIALS, CONFIGURATIONS AND SITE WORKS		
DESCRIPTION	QUANTITY	BIDDER'S STATEMENT OF COMPLIANCE
INTERNET DEDICATED SERVICE WITH HIGH-AVAILABILITY (HA)		
Independent ISP with modem / media converters	2	
Managed Telco Grade Router	2	
Bandwidth Manager Internet Access Gateway	1	
PABX System		
MANAGED PABX SYSTEM - 10SIP x 25 IP PHONES		
10 Vocoder Channels for SIP Trunks	1	
25 IP Subscriber Licenses		
1 Operator IP Phone w/ DSS Console		
24 Business IP Phones		
VMS for Automated Attendant		
SMDR Feature for Call Detail Records		
2 x 24-Port PoE Switch for IP Phones		
Installation, Testing, Commissioning and Acceptance		
Comprehensive Warranty & Support		
Project Acceptance and Turn-over		
1x Fiber 1 LEC 10MB - for remote extension within the building up (comes with wifi Router (4 Port), /29 IP Block, 1GB of either email or web Hosting Service and MRTG Access)		
NETWORK		
Supply of Equipment and Peripherals		
Core Switch	1	
24-Port Gigabit PoE Switch	2	
48-Port Gigabit Switch	4	
Cisco Meraki MR44 w/ MR Enterprise License, 1YR	10	
10G Transceiver Module	12	
Nagios XI Enterprise 100 Node License, 1 Year Ticket Support and Maintenance Plan	1	
2KVA UPS, Rackmount	2	
Site Supervision, Engineering and Project Management		
Preliminary Activities	1	
Supply of Labor and Manpower		
General Provision, Mobilization and Demobilization		
Physical Installation of Active Equipment		
Active Components System Configuration,		

Testing, and Commissioning		
Network Monitoring Software Installation & Commissioning		
Functionality Testing & UAT		
Configuration Validation / Host		
Provisioning of Temporary Tools and Equipment during installation		
End-user Training & Knowledge Transfer		
Project Documentation		
Project Turn-over		
Project Acceptance		
1- Year Maintenance Agreement		
1 -Year Standard Warranty		
STRUCTURED CABLING		
Supply of Network Peripherals and Cabling Components		
CAT6 UTP 4 PAIR SOLID 305M	3	
CAT6 24 Port UTP Patch Panel 1U	1	
Cable Boot (Black, Blue, Green, Gray, White, Yellow, Red)	20	
CAT6 Modular Plug / RJ45 Connector - Unshielded	20	
UTP Cable Management Guide 1U (Plastic)	10	
CAT6 UTP Patch Cord, 5M	100	
CAT6 UTP Patch Cord, 2M	100	
CAT6 UTP Patch Cord, 1M	20	
19" Open Bay Rack, 7 ft. w/ vertical cable manager	1	
Supply of Roughing-ins		
Roughing-in Materials, Fittings & Supports (Conduits, Mouldings, etc.)	1	
Consumables and Miscellaneous		
Site Supervision, Engineering and Project Management		
Preliminary Activities		
Supply of Labor and Manpower		
Mobilization and Demobilization		
Layout and Installation of Roughing-Ins		
UTP Cable Layout and Installation		
Port Testing, Re-tagging and Labelling (100 Ports)		
Termination of UTP Cables	1	
Re-patching of Existing Cabling		
Provisioning of Temporary Tools and Equipment during installation		
Project Documentation		
Project Turn-over		
Project Acceptance		
6-Months Workmanship Warranty on Cabling		

Works		
LOAD BALANCER		
Hardware appliance, 6 x GE RJ45 + 2 x SFP, 1 x available NIC slot, Default with 64GB SSD. Support 12Gbps Firewall Throughput, 4.2Gbps Threat Prevention Throughput	1	
System License Package for the following features: Firewall, Bandwidth Management, URL Filtering, Application Control	1	
System On-site Configuration of Supplied Equipment	1	
Testing & Commissioning		
System Training		
1-Year Equipment Warranty and Technical Support		

In the event that any of the materials run out, it shall be the responsibility of the winning bidder to replenish the same, notwithstanding from the quantity of the bill of materials.

A. WARRANTY AGAINST BENEFITS

The winning supplier warrants that it has not given nor promised to give any money or gift to any officer or employee of the PTA, or any member of the Bids and Awards Committee, BAC secretariat, or TWG, to secure this contract.

B. ASSIGNMENT

Unless otherwise expressly stipulated or prior written approval of the PTA is secured, this contract or any portion thereof shall not be assigned or subjected to any other party or parties.

I hereby certify that the statement of compliance to the foregoing technical specifications are true and correct, otherwise, if found to be false either during bid evaluation or post-qualification, the same shall give rise to automatic disqualification of our bid.

Name of Company

Signature Over Printed
Name of Authorized
Representative

Date

Section VIII. Checklist of Technical and Financial Documents

Notes on the Checklist of Technical and Financial Documents

The prescribed documents in the checklist are mandatory to be submitted in the Bid, but shall be subject to the following:

- a. GPPB Resolution No. 09-2020 on the efficient procurement measures during a State of Calamity or other similar issuances that shall allow the use of alternate documents in lieu of the mandated requirements; or
- b. Any subsequent GPPB issuances adjusting the documentary requirements after the effectivity of the adoption of the PBDs.

The BAC shall be checking the submitted documents of each Bidder against this checklist to ascertain if they are all present, using a non-discretionary "pass/fail" criterion pursuant to Section 30 of the 2016 revised IRR of RA No. 9184.

Checklist of Technical and Financial Documents

I. TECHNICAL COMPONENT ENVELOPE

Class "A" Documents

Legal Documents

- (a) Valid PhilGEPS Registration Certificate (Platinum Membership) (all pages) in accordance with Section 8.5.2 of the IRR;

Technical Documents

- (b) Statement of the prospective bidder of all its ongoing government and private contracts, including contracts awarded but not yet started, if any, whether similar or not similar in nature and complexity to the contract to be bid; **and**
- (c) Statement of the bidder's Single Largest Completed Contract (SLCC) similar to the contract to be bid, except under conditions provided for in Sections 23.4.1.3 and 23.4.2.4 of the 2016 revised IRR of RA No. 9184, within the relevant period as provided in the Bidding Documents; **and**
- (d) Original copy of Bid Security. If in the form of a Surety Bond, submit also a certification issued by the Insurance Commission;
or
Original copy of Notarized Bid Securing Declaration; **and**
- (e) Conformity with the Technical Specifications, which may include production/delivery schedule, manpower requirements, and/or after-sales/parts, if applicable; **and**
- (f) Original duly signed Omnibus Sworn Statement (OSS);
and if applicable, Original Notarized Secretary's Certificate in case of a corporation, partnership, or cooperative; or Original Special Power of Attorney of all members of the joint venture giving full power and authority to its officer to sign the OSS and do acts to represent the Bidder.

Financial Documents

- (g) The prospective bidder's computation of Net Financial Contracting Capacity (NFCC);
or
A committed Line of Credit from a Universal or Commercial Bank in lieu of its NFCC computation.

Class "B" Documents

- (h) If applicable, a duly signed joint venture agreement (JVA) in case the joint venture is already in existence;
or
duly notarized statements from all the potential joint venture partners stating that they will enter into and abide by the provisions of the JVA in the instance that the bid is successful.

Other documentary requirements under RA No. 9184 (as applicable)

- (i) [For foreign bidders claiming by reason of their country's extension of reciprocal rights to Filipinos] Certification from the relevant government

- office of their country stating that Filipinos are allowed to participate in government procurement activities for the same item or product.
- (j) Certification from the DTI if the Bidder claims preference as a Domestic Bidder or Domestic Entity.

25 FINANCIAL COMPONENT ENVELOPE

- (a) Original of duly signed and accomplished Financial Bid Form; and
- (b) Original of duly signed and accomplished Price Schedule(s).

Bid Form

Date: _____
 Invitation to Bid No: PB No. 23-08-2

*To: Philippine Tax Academy
 7th Floor EDPG Building,
 BSP Complex, Roxas Boulevard
 Malate, Manila*

Gentlemen and/or Ladies:

Having examined the Bidding Documents including Bid Bulletin Numbers [____], the receipt of which is hereby duly acknowledged, we, the undersigned, offer to Supply, Deliver, Install and Configure Next Generation Firewall Appliance and Internet Dedicated Service (IDS), and related services for the Philippine Tax Academy (PTA) in conformity with the said Bidding Documents.

Lot No.	Qty/Unit	ITEMS/ DESCRIPTION	UNIT PRICE	TOTAL PRICE
1	1 lot	Next Generation Firewall Appliance		
2	1 lot	High Availability (HA) Network Solution		
		Internet Dedicated Services with High Availability		
		Managed Service - PABX System,		
		Wireless Access Points with Cloud-based Management and Administration		
		Structured Cabling - Voice and Data		
TOTAL BID:				

Note: For purposes of bid evaluation, bidders are advised to use two (2) decimal places in setting up their bid prices.

TOTAL PRICE IN WORDS:

Lot 1: _____

Lot 2: _____

✓

We undertake, if our Bid is accepted, to deliver the goods in accordance with the delivery schedule specified in the Section VI. Schedule of Requirements.

If our Bid is accepted, we undertake to provide a performance security in the form, amounts, and within the times specified in the Bidding Documents.

We agree to abide by this Bid for the Bid Validity Period specified in BDS provision for ITB Clause 14.2 and it shall remain binding upon us and may be accepted at any time before the expiration of that period.

Until a formal Contract is prepared and executed, this Bid, together with your written acceptance thereof and your Notice to Proceed, shall be binding upon us.

We understand that you are not bound to accept the Lowest Calculated Bid or any Bid you may receive.

We certify/confirm that we comply with the eligibility requirements as per ITB Clause 5 of the Bidding Documents.

I/We likewise certify/confirm that the undersigned, *[for sole proprietorships, insert]*: as the owner and sole proprietor or authorized representative of *[Name of Bidder]*, has the full power and authority to participate, submit the bid, and to sign and execute the ensuing contract, on the latter's behalf for the Supply, Deliver, Install and Configure Next Generation Firewall Appliance and Internet Dedicated Service (IDS), and related services for the Philippine Tax Academy (PTA).

Or:

I/We likewise certify/confirm that the undersigned, *[for partnerships, corporations, cooperatives, or joint ventures, insert]*: is granted full power and authority by the *[Name of Bidder]*, to participate, submit the bid and to sign and execute the ensuing contract on the latter's behalf for Supply, Deliver, Install and Configure Next Generation Firewall Appliance and Internet Dedicated Service (IDS), and related services for the Philippine Tax Academy (PTA).

We acknowledge that failure to sign each and every page of this Bid Form, including the attached Schedule of Prices, shall be a ground for the rejection of our bid.

Dated this _____ day of _____ 20_____

[signature]

[in the capacity of]

Duly authorized to sign Bid for and on behalf of _____

W

Schedules of Prices for Goods Offered from Abroad

[shall be submitted with the Bid if bidder is offering goods from Abroad]

For Goods Offered from Abroad

Name of Bidder _____ Project ID No. _____ Page _____ of _____

1	2	3	4	5	6	7	8	9
Lot No.	Description	Country of origin	Quantity	Unit price CIF port of entry (specify port) or CIF named place (specify border point or place of destination)	Total CIF or CIF price per item (col. 4 x 5)	Unit Price Delivered Duty Unpaid (DDU)	Unit price Delivered Duty Paid (DDP)	Total Price delivered DDP (col 4 x 8)

Name: _____
 Legal Capacity: _____
 Signature: _____
 Duly authorized to sign the Bid for and behalf of: _____

mb

Schedule of Prices for Goods Offered from Within the Philippines
[shall be submitted with the Bid if bidder is offering goods from within the Philippines]

For Goods Offered from Within the Philippines

Name of Bidder _____ Project ID No. _____ Page _____ of _____

1	2	3	4	5	6	7	8	9	10
Lot No.	Description	Country of origin	Quantity	Unit price EXW per item	Transportation and all other costs incidental to delivery, per item	Sales and other taxes payable if Contract is awarded, per item	Cost of Incidental Services, if applicable, per item	Total Price, per unit (col 5+6+7+8)	Total Price delivered Final Destination (col 9) X (col 4)

Name: _____
 Legal Capacity: _____
 Signature: _____
 Authorized to sign the Bid for and behalf of: _____



Omnibus Sworn Statement (Revised)

[shall be submitted with the Bid]

REPUBLIC OF THE PHILIPPINES)
CITY/MUNICIPALITY OF _____) S.S.

AFFIDAVIT

I, [Name of Affiant], of legal age, [Civil Status], [Nationality], and residing at [Address of Affiant], after having been duly sworn in accordance with law, do hereby depose and state that:

1. *[Select one, delete the other:]*

[If a sole proprietorship:] I am the sole proprietor or authorized representative of [Name of Bidder] with office address at [address of Bidder];

[If a partnership, corporation, cooperative, or joint venture:] I am the duly authorized and designated representative of [Name of Bidder] with office address at [address of Bidder];

2. *[Select one, delete the other:]*

[If a sole proprietorship:] As the owner and sole proprietor, or authorized representative of [Name of Bidder], I have full power and authority to do, execute and perform any and all acts necessary to participate, submit the bid, and to sign and execute the ensuing contract for [Name of the Project] of the [Name of the Procuring Entity], as shown in the attached duly notarized Special Power of Attorney;

[If a partnership, corporation, cooperative, or joint venture:] I am granted full power and authority to do, execute and perform any and all acts necessary to participate, submit the bid, and to sign and execute the ensuing contract for [Name of the Project] of the [Name of the Procuring Entity], as shown in the attached [state title of attached document showing proof of authorization (e.g., duly notarized Secretary's Certificate, Board/Partnership Resolution, or Special Power of Attorney, whichever is applicable)];

3. [Name of Bidder] is not "blacklisted" or barred from bidding by the Government of the Philippines or any of its agencies, offices, corporations, or Local Government Units, foreign government/foreign or international financing institution whose blacklisting rules have been recognized by the Government Procurement Policy Board, **by itself or by relation, membership, association, affiliation, or controlling interest with another blacklisted person or entity as defined and provided for in the Uniform Guidelines on Blacklisting;**

4. Each of the documents submitted in satisfaction of the bidding requirements is an authentic copy of the original, complete, and all statements and information provided therein are true and correct;

5. [Name of Bidder] is authorizing the Head of the Procuring Entity or its duly authorized representative(s) to verify all the documents submitted;

6. *[Select one, delete the rest:]*

[If a sole proprietorship:] The owner or sole proprietor is not related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

[If a partnership or cooperative:] None of the officers and members of [Name of Bidder] is related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project

cd

consultants by consanguinity or affinity up to the third civil degree;

[If a corporation or joint venture:] None of the officers, directors, and controlling stockholders of *[Name of Bidder]* is related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

7. *[Name of Bidder]* complies with existing labor laws and standards;
8. *[Name of Bidder]* is aware of and has undertaken the responsibilities as a Bidder in compliance with the Philippine Bidding Documents, which includes:
 - a. Carefully examining all of the Bidding Documents;
 - b. Acknowledging all conditions, local or otherwise, affecting the implementation of the Contract;
 - c. Making an estimate of the facilities available and needed for the contract to be bid, if any; and
 - d. Inquiring or securing Supplemental/Bid Bulletin(s) issued for the *[Name of the Project]*.
9. *[Name of Bidder]* did not give or pay directly or indirectly, any commission, amount, fee, or any form of consideration, pecuniary or otherwise, to any person or official, personnel or representative of the government in relation to any procurement project or activity;
10. **In case advance payment was made or given, failure to perform or deliver any of the obligations and undertakings in the contract shall be sufficient grounds to constitute criminal liability for Swindling (Estafa) or the commission of fraud with unfaithfulness or abuse of confidence through misappropriating or converting any payment received by a person or entity under an obligation involving the duty to deliver certain goods or services, to the prejudice of the public and the government of the Philippines pursuant to Article 315 of Act No. 3815 s. 1930, as amended, or the Revised Penal Code;**
11. *[Name of Bidder]* hereby assigns the following contact number/s and e-mail address/es as the official telephone/fax number and contact reference of the company where the PTA BAC and PTA notices may be transmitted.

Telephone No/s.: _____
Fax No/s.: _____
E-mail Add/s.: _____
Mobile No.: _____

It is understood that notices/s transmitted in any of the above-stated telephone/fax numbers and/or e-mail address/es are deemed received as of its transmittal and the reckoning period for the reglementary periods stated in the bidding documents and the 2016 revised Implementing Rules and Regulations of Republic Act No. 9184 shall commence from receipt thereof.

IN WITNESS WHEREOF, I have hereunto set my hand this ___ day of ___, 20__ at _____, Philippines.

Bidder's Representative/Authorized Signatory



SUBSCRIBED AND SWORN to before me this ___ day of [month] [year] at [place of execution], Philippines. Affiant/s known to me, and known to be the same person/s in the exhibited [insert type of government identification card used*], with his/her photograph and signature appearing thereon, with no. _____ issued on _____ at _____.

Witness my hand and seal this ___ day of [month] [year].

NAME OF NOTARY PUBLIC
Serial No. of Commission
Notary Public for _____ until
Roll of Attorney's No.
PTR No. _____ [date issued],
[place issued]
IBP No. _____ [date issued],
[place issued]

Doc. No. _____
Page No. _____
Book No. _____
Series of _____

*The identification card shall be at least one of those acceptable proofs of identity as identified under the provisions of the 2004 Rules on Notarial Practice.

*"Sec. 12. Competent Evidence of Identity – The phrase "competent evidence of identity" refers to the identification of an individual based on:
At least one current identification document issued by an official agency bearing the photograph and signature of the individual, such as but not limited to, passport, driver's license, Professional Regulations Commission ID, National Bureau of Investigation clearance, police clearance, postal ID, voter's ID, Barangay certification, Government Service and Insurance System (GSIS) e-card, Social Security System (SSS) card, Philhealth card, senior citizen card, Overseas Workers Welfare Administration (OWWA) ID, OFW ID, seaman's book, alien certificate of registration/immigrant certificate of registration, government office ID, certification from the National Council for the Welfare of Disabled Persons (NCWDP), Department of Social Welfare and Development (DSWD) certification;*

The Board Resolution or Secretary's Certificate referring to the said Board Resolution designating the bidder's authorized representative and signatory need not specifically indicate the particular project where such authority is given provided that the said authority covers activities by PTA.



JOINT VENTURE AGREEMENT

KNOW ALL MEN BY THESE PRESENTS:

This **JOINT VENTURE AGREEMENT** (hereinafter referred to as the "Agreement"), entered into this _____ day of _____ 20__ at _____ City, Philippines by and among:

_____, A domestic corporation duly organized, registered and existing under and by virtue of the laws of the Republic of the Philippines, with office address at _____, represented by its _____, hereinafter referred to as "_____";

- and -

_____, A domestic corporation duly organized, registered and existing under and by virtue of the laws of the Republic of the Philippines, with office address at _____,

_____, represented by its _____, hereinafter referred to as "_____";

- and -

_____ a foreign corporation organized and existing under and by virtue of the laws of _____, represented by its _____, hereinafter referred to as "_____";

(Henceforth collectively referred to as the "Parties")

WITNESSETH: That

WHEREAS, the Procurement Service (PS) has recently published an Invitation to Apply for Eligibility and to Bid for the Supply and Delivery of _____ for the _____;

mo

WHEREAS, the parties have agreed to pool their resources together to form the
"_____ Joint Venture", hereinafter referred to as the Joint Venture, under the laws of
the Philippines, for the purpose of participating in the abovementioned procurement of PS-DBM;

NOW, THEREFORE, for and in consideration of the foregoing premises and the covenants
hereto set forth, the Parties have agreed as follows:

ARTICLE I ORGANIZATION OF THE JOINT VENTURE

SECTION 1. Formation – The Parties do hereby agree and bind themselves to establish, form and
organize a Joint Venture pursuant to the laws of the Republic of the Philippines, in order for the JV to
carry on the purposes and objectives for which it is created;

SECTION 2. Name – The name and style under which the JV shall be conducted is "_____";

SECTION 3. Principal Place of Business – The JV shall maintain its principal place of business at
_____;

SECTION 4. Preparation and Documentation – The Parties shall secure and/or execute such
certifications, documents, deeds and instruments as may be required by the laws of the Republic of the
Philippines for the realization of the JV and in compliance with the Project. Further, they shall do all
other acts and things requisite for the continuation of the JV pursuant to applicable laws;

SECTION 5. The Joint Venture shall be represented by the _____ in all biddings, related procurement
transactions and other official dealings that it shall enter into with the PTA, such transactions to include, among
others, the submission of eligibility documents, bids, registration documents obtaining bonds, performing the
principal contract in the event that the contract is awarded in favor of the Joint Venture, receipt of payment for
goods delivered, and similar and related activities.

SECTION 6. The period of the Joint Venture shall begin upon execution of this Agreement and shall continue
until the complete performance of its contractual obligations to PTA, as described in Article II hereof, or upon its
termination for material breach of any term or condition of this Agreement, by service of a written statement in
English on the other Party, not less than 90 days prior to the intended date termination

**ARTICLE II
PURPOSE**

SECTION 1. The primary purpose of the Joint Venture is to participate in the public bidding to be conducted by the PTA Bids and Awards Committee for the supply and delivery of _____ for the _____.

SECTION 2. If the above-described contract/s is/are awarded to the Joint Venture, the Joint Venture shall undertake the performance thereof to PTA, and such other incidental activities necessary for the completion of its contractual obligations.

**ARTICLE III
SOLIDARY LIABILITY OF THE PARTIES**

SECTION 1. In the performance of the contract/s that may be awarded to the Joint Venture by the PS-DBM, and all other related activities/obligations, as described in Article II hereof, the Parties bind themselves jointly and solidarily, in the concept of solidarily debtors, subject to the right of reimbursement, as provided in the relevant provisions of the Civil Code of the Philippines.

**ARTICLE IV
CONTRIBUTION AND OTHER ARRANGEMENTS**

SECTION 1. Contribution – The Parties shall contribute the amount of _____ (Php) to support the financial requirements of the Joint Venture, in the following proportion:

A.	-	P	.00
B.	-	P	.00
TOTAL		P	.00

Additional contributions to the Joint Venture shall be made as may be required for contract implementation. In addition, _____ shall contribute any labor and contract management requirements.

SECTION 2. Profit Sharing – The share of the Parties to the JV from any profit derived or obtained from the implementation and execution of the Project shall be distributed pro rata to each, in accordance with the contribution and resources each has provided to the JV;

SECTION 3. Liquidation and Distributions – Any sum remaining after deducting from the total of all moneys or benefits received for the performance of the contract, all costs incurred by the JV after award of the contract for the Project pursuant to the accounting practices established for the JV, shall be distributed in accordance with the relative balances in the accounts of each Party pursuant to Sec. 1 of this Article upon completion, final accounting, termination and liquidation of the JV. In the event of liquidation and termination of JV, and after taking into account the shares of the Parties in all income, gain, deductions, expenses, and losses, should the account of a Party contain a negative balance, such Party shall contribute cash to the JV sufficient to restore the said balance to zero;

SECTION 4. Sharing of Burden of a Net Loss – In case a net loss is incurred, additional contributions shall be made by the Parties in accordance with their respective shares.

**ARTICLE V
MISCELLANEOUS PROVISIONS**

SECTION 1. The provisions of the Instructions to Bidders, Supplemental Bid Bulletin, and other bidding documents issued by the PTA in relation to the contract described in Article II hereof, shall be deemed incorporated in this Agreement and made an integral part thereof.

SECTION 2. This Agreement shall be binding upon and inure to the benefit of the Parties and their respective successors and assigns.

SECTION 3. The Parties herein are duly represented by their authorized officers.

SECTION 4. Governing Law – This Agreement shall be governed by and construed according to the laws of the Republic of the Philippines. Venue of any court action arising from this Agreement shall be exclusively laid before the proper court of the _____, Philippines.

IN WITNESS WHEREOF, the parties have set their hands and affixed their signatures on the date and place first above-stated.

Signed in the Presence of:

ms

ACKNOWLEDGMENT

REPUBLIC OF THE PHILIPPINES)
CITY/MUNICIPALITY OF _____) S.S.
PROVINCE OF (in the case of Municipality)

BEFORE ME, a Notary Public for and in the City/Municipality of _____ (indicate also the Province in the case of Municipality), this _____ day of _____ (month & year) _____ personally appeared the following:

Name ID Name, Number and Validity Date

Known to me and to me known to be the same persons who executed the foregoing instrument and they acknowledge to me that the same is their free and voluntary act and deed and that of the corporation(s) they represent.

This instrument refers to a Joint Venture Agreement consisting of _____ pages, including the page on which this Acknowledgement is written, and signed by the parties and their instrumental witnesses.

WITNESS MY HAND AND NOTARIAL SEAL on the place and on the date first above written.

NAME OF NOTARY PUBLIC

Serial No. of Commission _____
Notary Public for _____ until _____
Roll of Attorneys No. _____
PTR No. __, [date issued], [place issued]
IBP No. __, [date issued], [place issued]

Doc. No. ____
Page No. ____
Book No. ____
Series of ____.

Note:

The identification card shall be at least one of those acceptable proofs of identity as identified under the provisions of the 2004 Rules on Notarial Practice.

"Sec. 12. Competent Evidence of Identity – The phrase "competent evidence of identity" refers to the identification of an individual based on:

At least one current identification document issued by an official agency bearing the photograph and signature of the individual, such as but not limited to, passport, driver's license, Professional Regulations Commission ID, National Bureau of Investigation clearance, police clearance, postal ID, voter's ID, Barangay certification, Government Service and Insurance System (GSIS) e-card, Social Security System (SSS) card, Philhealth card, senior citizen card, Overseas Workers Welfare Administration (OWWA) ID, OFW ID, seaman's book, alien certificate of registration/immigrant certificate of registration, government office ID, certification from the National Council for the Welfare of Disabled Persons (NCWDP), Department of Social Welfare and Development (DSWD) certification

SUPPLIER'S LETTERHEAD

Date

**Chairperson
PTA Bids and Awards Committee
EDPC Bldg. BSP Complex,
Roxas Boulevard, Malate, Manila**

Dear Sir/Mam:

This has reference to Public Bidding No. _____ for _____ (Name of Project) _____,
_____ (Name of Company) _____ respectfully requests for the following:

- Withdraw of Bid Submissions
 - Refund of Bid Security
- (Attached is a photocopy of the Philippine Tax Academy Official Receipt)

It is understood that _____ waives its right to file any motion for reconsideration and/or protest in connection with the above-cited Public Bidding Project.

Thank you.

Very truly yours,

Authorized Signatory for the Company

ms

BID SECURING DECLARATION FORM

REPUBLIC OF THE PHILIPPINES)
CITY OF _____) S.S.

x-----x

BID SECURING DECLARATION
Invitation to Bid: *Public Bidding No. 23-08-2*

To: *Philippine Tax Academy*
PTA Bids and Awards Committee
EDPC Bldg., BSP Complex,
Roxas Boulevard, Malate, Manila

I/We³, the undersigned, declare that:

1. I/We understand that, according to your conditions, bids must be supported by a Bid Security, which may be in the form of a Bid-Securing Declaration.
2. I/We accept that: (a) I/we will be automatically disqualified from bidding for any contract with any procuring entity for a period of two (2) years upon receipt of your Blacklisting order; and, (b) I/we will pay the applicable fine provided under Section 6 of the Guidelines on the Use of Bid Securing Declaration, within fifteen (15) days from receipt of the written demand by the procuring entity for the commission of acts resulting to the enforcement of the bid securing declaration under Sections 23.1(b), 34.2, 40.1 and 69.1, except 69.1(f), of the IRR of RA 9184; without prejudice to other legal action the government may undertake.
3. I/We understand that this Bid Securing Declaration shall cease to be valid on the following circumstances:
 - a. Upon expiration of the bid validity period, or any extension thereof pursuant to your request;
 - b. I am/we are declared ineligible or post-disqualified upon receipt of your notice to such effect, and (i) I/we failed to timely file a request for reconsideration or (ii) I/we filed a waiver to avail of said right;
 - c. I am/we are declared the bidder with the Lowest Calculated Responsive Bid, and I/we have furnished the performance security and signed the Contract.

IN WITNESS WHEREOF, I/We have hereunto set my/our hand/s this ____ day of [month] [year]
at [place of execution].

³ Select one and delete the other. Adopt the same instruction for similar terms throughout the document.



[Insert NAME OF BIDDER'S AUTHORIZED REPRESENTATIVE]
[Insert Signatory's Legal Capacity]

Affiant

SUBSCRIBED AND SWORN to before me this ___ day of [month] [year] at [place of execution], Philippines. Affiant/s known to me, and known to be the same person/s in the exhibited [insert type of government identification card used*], with his/her photograph and signature appearing thereon, with no. _____ issued on _____ at _____.

Witness my hand and seal this ___ day of [month] [year].

NAME OF NOTARY PUBLIC _____
Serial No. of Commission _____
Notary Public for _____ until _____
Roll of Attorney's No. _____
PTR No. _____ [date issued], [place issued]
IBP No. _____ [date issued], [place issued]

Doc. No. _____
Page No. _____
Book No. _____
Series of _____

**The identification card shall be at least one of those acceptable proofs of identity as identified under the provisions of the 2004 Rules on Notarial Practice.*

"Sec. 12. Competent Evidence of Identity – The phrase "competent evidence of identity" refers to the identification of an individual based on:

At least one current identification document issued by an official agency bearing the photograph and signature of the individual, such as but not limited to, passport, driver's license, Professional Regulations Commission ID, National Bureau of Investigation clearance, police clearance, postal ID, voter's ID, Barangay certification, Government Service and Insurance System (GSIS) e-card, Social Security System (SSS) card, Philhealth card, senior citizen card, Overseas Workers Welfare Administration (OWWA) ID, OFW ID, seaman's book, alien certificate of registration/immigrant certificate of registration, government office ID, certification from the National Council for the Welfare of Disabled Persons (NCWDP), Department of Social Welfare and Development (DSWD) certification

nb

Performance Securing Declaration (Revised)

REPUBLIC OF THE PHILIPPINES)
CITY OF _____) S.S.

PERFORMANCE SECURING DECLARATION

Invitation to Bid: [Insert Reference Number indicated in the Bidding Documents]
To: [Insert name and address of the Procuring Entity]

I/We, the undersigned, declare that:

1. I/We understand that, according to your conditions, to guarantee the faithful performance by the supplier/distributor/manufacture/contractor/consultant of its obligations under the Contract, I/we shall submit a Performance Securing Declaration within a maximum period of ten (10) calendar days from the receipt of the Notice of Award prior to the signing of the Contract.
2. I/We accept that: I/we will be automatically disqualified from bidding for any procurement contract with any procuring entity for a period of one (1) year for the first offense, or two (2) years **for the second offense**, upon receipt of your Blacklisting Order if I/We have violated my/our obligations under the Contract;
3. I/We understand that this Performance Securing Declaration shall cease to be valid upon:
 - a. issuance by the Procuring Entity of the Certificate of Final Acceptance, subject to the following conditions:
 - i. Procuring Entity has no claims filed against the contract awardee;
 - ii. It has no claims for labor and materials filed against the contractor; and
 - iii. Other terms of the contract; or
 - b. replacement by the winning bidder of the submitted PSD with a performance security in any of the prescribed forms under Section 39.2 of the 2016 revised IRR of RA No. 9184 as required by the end-user.

IN WITNESS WHEREOF, I/We have hereunto set my/our hand/s this ____ day of [month] [year] at [place of execution].

[Insert NAME OF BIDDER'S AUTHORIZED
REPRESENTATIVE]
[Insert Signatory's Legal Capacity]
Affiant

SUBSCRIBED AND SWORN to before me this ____ day of [month] [year] at [place of execution], Philippines. Affiant/s known to me, and known to be the same person/s in the exhibited [insert type of government identification card used*], with his/her photograph and signature appearing thereon, with no _____ issued on _____ at _____.

Republic of the Philippines



Government Procurement Policy Board