

**TERMS OF REFERENCE
FOR
SUPPLY, DELIVERY, INSTALLATION, TESTING, TRAINING AND
COMMISSIONING OF ICT EQUIPMENT AND SOFTWARE FOR UPGRADING
NETWORK FOR WFFC AND CENTRAL OFFICE**

A. BACKGROUND

The planned upgrade of network equipment and peripherals for WFFC (Weather and Flood Forecasting Center), and Central Office, coupled with comprehensive security training, marks a significant stride towards establishing a more secure and resilient ICT environment for PAGASA. This initiative is not only critical for enhancing the overall efficiency and reliability of our technological infrastructure but also for safeguarding sensitive meteorological data and communication channels.

By modernizing our network hardware, we aim to eliminate outdated systems that may be vulnerable to cyber threats and performance issues. The introduction of cutting-edge firewalls for our site-to-site VPN will significantly improve data transmission speeds, reduce latency, and ensure robust network security. These upgrades will enable us to handle the increasing volume of meteorological data with greater accuracy and speed, facilitating more timely and precise weather forecasting and flood control measures.

In parallel, the implementation of a rigorous training program focused on cybersecurity best practices will empower our staff with the knowledge and skills necessary to protect against evolving cyber threats. This training will cover essential topics such as recognizing phishing attempts, securing personal devices, and responding to potential security breaches. By fostering a culture of security awareness, we can mitigate the risk of human error, which is often a significant factor in cybersecurity incidents. Moreover, the training will be tailored to address the specific needs and challenges faced by PAGASA, ensuring that ICT personnel are well-prepared to contribute to the organization's overall security posture.

B. APPROVED BUDGET FOR THE CONTRACT (ABC)

The Approved Budget for the Contract (ABC) is distributed as follows:

LOT	ITEM	ABC
A	SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION, COMMISSIONING & TRAINING OF INTEGRATED FIREWALL SOLUTION AND SOFTWARE DEVELOPMENT	7,700,000.00

B	SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION, COMMISSIONING & TRAINING RACK MOUNT SERVER	2,300,000.00
----------	--	---------------------

The total ABC for the project is **Ten Million Pesos (10,000,000.00)** inclusive of VAT and all applicable government taxes.

This procurement is on a per lot basis. Bidders can offer any or all of the lots. Evaluation and award are on a per lot basis.

C. QUALIFICATIONS OF THE BIDDER

(Please refer to Section II. Instructions to Bidders, the Bid Data Sheet and Checklist of Eligibility and Technical Requirements of the Bidding Documents)

D. DELIVERY PERIOD AND PLACE OF DELIVERY

The winning bidder shall supply, deliver, install, test, commission, and train components of the project on the fourth floor in the ICT room at PAGASA Central Office Building, Science Garden Complex, Senator Miriam P. Defensor-Santiago Avenue, Barangay Central, Quezon City within the period of **One Hundred Twenty (120) calendar days** from receipt of the Notice to Proceed (NTP).

E. BID PROPOSAL CONTENTS

The prospective bidder is expected to comply and respond in accordance with the specific instructions to bidders and submit all the documentary requirements under the Checklist of Eligibility, Technical and Financial Requirements. The submission of documentary requirements must be properly arranged in order and with labels.

The prospective bidder shall respond paragraph by paragraph and shall clearly indicate compliance to all the required specifications (*Please see Section VII. Compliance Matrix*) and shall specify the number of days or schedules within which to complete the delivery of all the goods required (*Please see Section VI. Schedule of Requirements*).

The prospective bidder shall also be required to include in this proposal, original descriptive literature and un-amended brochures of all equipment/materials to be supplied. Plans, drawings, and diagrams/configurations must likewise be provided.

These details will allow the **PAGASA-Bids and Awards Committee** to fully evaluate and determine compliance from the prospective bidders.

F. SYSTEM SOFTWARE AND HARDWARE SPECIFICATIONS

F.1.LOT A: SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION, COMMISSIONING & TRAINING OF INTEGRATED FIREWALL SOLUTION AND SOFTWARE DEVELOPMENT

The winning bidder shall supply, deliver, install, integrate, test and commission the Firewall Solution offered with the following minimum specifications:

F.1.1 Integrated Firewall Solution

The proposed solution must have at least the following specifications:

- Physical Interface
 - At least 6x 10/100/1000 BASE-T Interfaces
 - At least 4x10GE Fiber SFP+ Interfaces
 - At least 2x USB Ports
 - At least 1x Serial Port
- Performance
 - Firewall Throughput – 2.8 Gbps
 - NGFW Throughput – 2.5 Gbps
 - WAF Throughput – 2.5 Gbps
 - IPS & WAF Throughput -1.4 Gbps
 - Threat Protection Throughput -1.8Gbps
 - IPsec VPN Throughput - 250Mbps
 - Max IPsec VPN Tunnels – 300
 - Concurrent TCP Connections – 750,000
 - New TCP Connections – 20,000
- Hardware
 - RAM - 4GB
 - Storage HD Capacity – 64G SSD
 - Power - 40W
 - Operating Temperature - 0-45°C
- Must support policy configuration modules for the following functions from a single appliance:
 - IPsec Virtual Private Network (IPVPN)
 - Secure Sockets Layer Virtual Private Network (SSLVPN)
 - Proprietary Virtual Private Network (VPN)
 - Software-Defined Wide Area Network (SDWAN) Capability
 - Web Application Firewall (WAF)
 - Anti-Virus/Malware (AV)
 - Intrusion Prevention System (IPS)
 - Real-time Vulnerability Scanner
- Must provide an on-premise URL signature database for URL Filtering, not only rely on cloud
- Must support anti-virus feature that scan the files up to 20MB.
- Must support anti-virus feature with compressed file detection, and support compress file with up to 16 layers.
- Must provide risk analytics module that allows to scan and identify security loopholes such as open port, system vulnerabilities, weak passwords, etc.

"Tracking the sky...helping the country"

- Must have risk assessment that support major protocols such as HTTP, HTTPS, POP3, SMTP, RDP, SMB, Oracle, MSSQL, MySQL etc.
- Must include the local hard disk to provide log retention and report creation of at least 30 days
- Must have SD-WAN capability via VPN tunnels:
 - o Can provide intelligent or dynamic path selection
 - o Can choose the optimize link based on bandwidth-remaining ratio, application type or link quality (means packet loss, jitter, latency).
- Must able to support multiple ISPs for SD-WAN.
- Must support WAF feature by itself, without additional devices. The WAF protection should meet at least the following specifications:
 - o Must be able to support the attack types, such as XSS, SQL, CSRF, CC attack, OS Command Injection, Web shell, scanner blocker, path transversal etc.
 - o Be able to defense OWASP top 10 attacks
 - o Support WAF related signature on premise no less than 4500 signatures and support customize signature.
 - o Support HTTPS site protection with decryption enabled.
 - o Support weak password detection for web-based applications.
 - o Support CC attack protection
 - o Support HTTP request Anomaly detection, SQL injection in HTTP header, POST entity overflow, HTTP header overflow, etc.
- Must provide a real-time vulnerability analysis or passive vulnerability scan:
 - o Detection vulnerabilities based on traffic pass through, without any active scanning activities to the servers, minimize the extra work load and other impact
 - o The vulnerabilities that can be detected includes web application vulnerability, weak password, improper configuration on web server, etc.
 - o Support generate HTML format report
- Must support ACL policy optimizer, which helps:
 - o Identify the redundant policy, expired policy, conflict policy etc.
 - o Be able to track the ACL policy life cycle, help to track every change that have been done to the ACL policies.
- Must support a dedicated ransomware protection module, which can:
 - o Automatically scan and detect ransomware related vulnerabilities, port, weak password, brute-force attack etc.
 - o Provide dedicated GUI page to show and respond all the ransomware related vulnerabilities
 - o Can provide guidance or suggested action to admin, e.g., deploy block policy direct
- Must support a dedicated dashboard to summarize business system(server) relate security risks, the information provide via dashboard includes:
 - o Business system severity level, attack events, vulnerabilities.
 - o Stages of Attack to let IT admin understand the security impact
 - o One-click to block attackers IP
- Must support a dedicated dashboard to summarize user relate security risks, the information provide via dashboard includes:

"Tracking the sky...helping the country"

- o User severity level, attack types, attack events
- o Stages of Attack to let IT admin understand the security impact
- Must support building a proprietary virtual private network (VPN) tunnel with the existing Head Office Firewall to ensure the security, interoperability, and ease of management
- Must support implementing security policies coming from a central manager that can manage remote offices and the existing head office firewall thus ensuring compatibility and interoperability.
- To ensure the maturity of technology, the solution offer must be CMMI L5 certified
- The proposed solution must be in level of Magic Quadrant for Network Firewalls 2022.
- To ensure the maturity of technology, the solution offer must have the following certification:
 - o ISO 9001:2015
 - o ISO/IEC 27001:2013
 - o ISO 14001:2015
 - o ISO/IEC 20000-1:2018
- Partner/reseller for the proposed solution must have technical certification from the principal/vendor.
- The winning bidder must have a certified true copy of a valid certificate of distributorship/dealership/reseller ship or professional partnership with the distributor/manufacture of the brand for Integrated Firewall Solution offered
- Peripherals
 - o 2 x 10GB SFP+ Transceiver
- Inclusive of licenses for 1 year

F.1.2 Application Security Testing Platform

The proposed solution must have the following minimum specifications:

- The solution should detect web application vulnerabilities via crawl/application analysis, universal translator, normalization, pre-attack analysis, attack, and generating reports after the scan runs. Describe explicitly in details on how vulnerabilities are detected by the solution.
- The solution must provide coverage for the following technologies:
 - o REST, WSDL, JSON, GWT, JavaScript, Mobile, AJAX, HTML4, HTML5, Single Page Applications (SPAs), SOAP, .NET, Flash Remoting (AMF), Silverlight, Living in the DOM, Complex Sequences, CSRF / XSRF Token Tracking.
- The proposed solution should support minimally the below mentioned classes of security vulnerabilities:
 - o Anonymous Access, Apache Struts 2 Framework Checks, Apache Struts Detection, Arbitrary File Upload, autocomplete attribute, Browser Cache directive (web application performance), Browser Cache directive (leaking sensitive information), Blind SQL Injection, Brute Force (Form Auth), Brute Force (HTTP Auth),

Business logic abuse attacks, Clients Cross-Domain Policy Files, Collecting Sensitive Personal Information (Personal Sensitive Information), Cookie attributes, Content Security Policy Header, Command Injection, Credentials stored in clear text in a cookie, Credentials Over Insecure Channel, Cross-Site Request Forgery (CSRF), Cross-site scripting (XSS), DOM based, Cross-site scripting (XSS), reflected, Cross-site scripting (XSS), passive – XSS Persistent, Cross-site scripting (XSS), active – XSS PersistentActive , Cross-site tracing (XST), Cross Origin Resources Sharing (CORS), Directory Indexing, Email Disclosure, Expression Language Injection, File Inclusion, Forced Browsing, Form Session Strength, FrontPage Checks, Heartbleed Check, HTTP Authentication over insecure channel, HTTP Headers, HTTP Query Session Check, HTTP Response Splitting, HTTP Strict Transport Security, HTTP User-Agent Check, HTTP Verb Tampering (Request Method Tampering), HTTPS Downgrade, HTTPS Everywhere, LDAP Injection, Local Storage Usage, Information Disclosure, Information Leakage, Java Grinder, Nginx NULL code, NoSQLi Injection, OS Commanding, Out of Band Stored Cross-site scripting (XSS), Parameter Fuzzing, PHP Code Execution, Predictable Resource Location, Privilege Escalation, Privacy Disclosure, Profanity, Reflection, Remote File Include (RFI), Reverse Clickjacking, Reverse Proxy, Secure and non-secure content mix, Server Configuration, Server Side Include (SSI) Injection, Server Side Request Forgery, Session Fixation, Session Strength, Session Upgrade, Source Code Disclosure, SQL Injection, SQL injection Auth Bypass, SQL Information Leakage (SQL Errors), SQL Parameter Check, SSL Strength, Unvalidated Redirect, URL rewriting, Web Beacon, Web Service Parameter Fuzzing, X-Frame-Options missing HTTP header, X-Content-Type-Options, X-XSS-Protection missing HTTP header, XML External Entity Attack, XPath Injection.

- Solution Capabilities
 - The proposed solution should not control number of project/apps to be configured as long it falls within the solution licensing limit, i.e. FQDNs
 - The proposed solution should have options to reduce the risk that minimum disruptions to service are caused when testing/performed against production applications. Describe how can the solution achieve that.
 - The proposed solution should have ability for determining code coverage completeness of your testing solution - to understand and highlight areas of the application that were not covered with the testing. Describe how can the solution achieve that.
 - The proposed solution should have options for a "quick scan" to get started, determine correct functioning, and so on, versus a deep full scan? Describe how can the solution achieve that.
 - The proposed solution should have ability to allow mix of attack modules to be configure in a single attack template and allowing it to be reusable in different scan configuration with minimum changes. Describe how can the solution achieve that.

"Tracking the sky...helping the country"

- o The proposed solution should have ability to add context to your apps and vulnerabilities with context tagging
- o The proposed solution security testing should satisfy regulations and provides the below types of reports. Describe how can the solution achieve that.
- o Payment Card Industry (PCI), OWASP 2017, Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA), GDPR
- o The proposed solution security testing should provide high-level executive reporting summarizes the overall health through the analysis of vulnerability severity, type, status and a variety of other metrics. Below are the required health overview (but not-limited to): Scan Statistics, Top 10 Vulnerability Types, Most Common Vulnerability Severity, Most Common Vulnerability Status,
- o The proposed solution security testing should provide high-level overview of your apps and vulnerabilities, without using external tools. Below are the required overview (but not-limited to): Number of Apps, Scans and Vulnerabilities, Vulnerabilities By Status, Vulnerabilities By Severity, Apps With Most Vulnerabilities, Top Vulnerability Types, Running Scans, Failed Scans, Completed Scans, Scheduled Scans, Interrupted Scans, Scan Usage By Month, Apps Scanned This Month
- o The proposed solution should provide the ability to execute retests of single vulnerabilities against previously discovered items once they are believed to have been remediated.
- o The proposed solution should allow developers quickly replicate discovered vulnerability without retesting the entire application. Describe how can the solution achieve that.
- o The proposed solution should allow developers quickly compare attacks performed and highlight differences between them. Describe how can the solution achieve that.
- o The proposed solution should allow developers to edit parameters to request URL on the headers visually on editor before launching retest again. Describe how can the solution achieve that.
- o The proposed solution should provide a record or replay capability of vulnerabilities discovered so that the exploitation of a vulnerability can be replayed by the developer investigating the issue or later by information security to ensure the vulnerability has been addressed when retesting.
- o The proposed solution should support sequence auto detection and CSRF token detection. Describe how can the solution detect such.
- o The proposed solution should have ability to handle Single Page Application's (SPA's).
- o The proposed solution should support testing Flash remoting sites (AMF).
- Mobile Application Security Testing
 - o The proposed solution should have ability to test web applications designed for use on mobile device. Describe how the solution does that.

- o The proposed solution should have ability to analyze traffic between the mobile app and web server and/or ability to analyze web application/service that communicates with mobile app. Describe how the solution does that.
- o The proposed solution should have ability to traffic analysis mobile application. Describe the solution support that.
- Testing Accuracy and other types of scanning
 - o The proposed solution should demonstrate evidence that your vulnerability detection is accurate. How does the solution achieve;
 - o The proposed solution should ensure the testing accuracy to reduce false positives. Describe any specific techniques/tuning are applied;
 - o The proposed solution should ensure the testing accuracy to reduce false negatives. Describe any specific techniques/tuning are applied;
 - o The proposed solution should be safe to scan Production environments. Please describe what had been done in the solution to achieve that.
- Management Reporting and Analysis.
- Remediation Advice, Examples and Guidance.
- System Requirement and Maintenance.
- Must provide Product Market Position and Certification.
- The winning bidder must have a certified true copy of a valid certificate of distributorship/dealership/reseller ship or professional partnership with the distributor/manufacture of the brand for Application Security Testing Platform offered.
- 1 Year Subscription for 5 domains
- Must be inclusive of implementation Services
- 1 Year technical support services via email, phone, or SMS during work days

F.1.3 Incident Handling Engineer Training (Introductory Course)

The proposed training must have at least the following course objectives and offer:

- The training objective is to enhance the capabilities of PAGASA IT personnels in incident handling and response, ensuring they are well-prepared to protect organizational assets from cyber threats.
- Modules must include at least the following topics:
 - o What is an Incident
 - o What is Incident Handling
 - o Difference Between Incident Handling (IH) and Incident Response (IR) Section
 - o The Incident Response Process
 - o Incident Response Policy
 - o Incident Response Plan

- o Incident Response Models
- o Education and Awareness
- o Information Sharing
- o Threat Hunting
- o Threat Analysis Frameworks
- o Tools and Toolkits
- o Policy
- o Procedures
- o Signs of an Incident
- o Sources of Precursors and Indicators
- o Incident Analysis
- 10 ICT personnel (Face to Face)
- 5 Days Training (8 Hours per Day)
- Location: DOST PAGASA Central Office
- Inclusive of meals and snacks for the participants
- The training is intended for PAGASA IT managers in the area of:
 - o IT Security
 - o System Administration
 - o Network Administration
 - o Incident Response Team Members
 - o Other professionals involved or related to cybersecurity and incident response
- Training should utilize a combination of:
 - o Instructor-led sessions
 - o Interactive discussions
 - o Practical hands-on labs
 - o Assessment and feedback
- Qualification requirements
 - o The Trainer/Trainers must at least have an International Cybersecurity Certification such as (L|PT, ISC2 CISSP, CompTIA CASP+, ISACA CISM and Mile2 Certifications).
 - o The training provider must be in the service industry for at least 5 years.
 - o The training provider must be at least have a Mile2 Accredited Training Partner

F.1.4 CCNA 1: Intro to Networks (ITN) Training

This training course introduces the architecture, structure, functions, components, and models of the Internet and other computer networks.

- Modules must at least include the following topics:
 - o Networking Today
 - o Basic Switch and End Device Configuration
 - o Protocol Models
 - o Physical Layer
 - o Number Systems

- o Data Link Layer
- o Ethernet Switching
- o Network Layer
- o Address Resolution
- o Basic Router Configuration
- o IPv4 Addressing
- o IPv6 Addressing
- o ICMP
- o Transport Layer
- o Application Layer
- o Network Security Fundamentals
- o Build a Small Network
- At Least five (5) personnel from PAGASA ICT must be present
- Training must be conducted in person (Face to Face)
- Must have at least seventy (70) Hours, 10-day training workshop
- Meals, transportation allowance (if applicable), Training materials and certificates must be provided during the course duration.

F.1.5 CCNA 2: Switching, Routing and Wireless Essentials (SRWE) Training

- This course describes the architecture, components, and operations of routers and switches in a small network.
- Training modules must at least include the following topics:
 - o Basic Device Configuration
 - o Switching Concepts
 - o VLANs
 - o Inter-VLAN Routing
 - o STP
 - o EtherChannel
 - o DHCPv4
 - o SLAAC and DHCPv6 Concepts
 - o FHRP Concepts
 - o LAN Security Concepts
 - o Switch Security Configuration
 - o WLAN Concepts
 - o WLAN Configuration
 - o Routing Concepts
 - o IP Static Routing
 - o Troubleshoot Static and Default Routes
- At least six (6) personnel from PAGASA ICT must be present
- Training must be conducted in person (Face to Face)
- Must have at least seventy (70) Hours, 10-day training workshop
- Meals, transportation allowance (if applicable), Training materials and certificates must be provided during the course duration.

F.1.6 CCNA 3: Enterprise Networking, Security and Automation (ENSA) V7

- This course describes the architecture, components, and operations of routers and switches in larger and more complex networks.
- Training modules must at least include the following topics:

"Tracking the sky...helping the country"

- Single-Area OSPFv2 Concepts
- Single-Area OSPFv2 Configuration
- WAN Concepts
- Network Security Concepts
- ACL Concepts
- ACLs for IPv4 Configuration
- NAT for IPv4
- VPN and IPsec Concepts
- QoS Concepts
- Network Management
- Network Design
- Network Troubleshooting
- Network Virtualization
- Network Automation
- At least eight (8) personnel from PAGASA ICT must be present
- Training Must be conducted in person (face to face)
- Must have at least Seventy (70) Hours, Ten (10)-days training workshop
- At least eight (8) personnel from PAGASA ICT must be eligible to take the “Cisco Certified Network Associate (CCNA)” Certification Examination.
- Meals, transportation allowance (if applicable), Certification exam fee, Training materials and certificates must be provided during the course duration.

F.1.7 PAGASA Early Warning Mobile Application

The proposed solution must have the following minimum specifications:

- Cross platform mobile application (Android and IOS)
- Mobile application features
 - Thunderstorm Advisory/Warning
 - Rainfall Alert
 - Tropical Cyclone
 - General Flood Advisory
 - Key Cities 5-day Weather Outlook
 - Provincial Extended Weather Outlook
 - Lightning Alert
 - Heat Index
 - Key cities Percent Chance of Precipitation (POP)
 - The mobile app API will provide location-specific weather data along with detailed instructions and safety guidelines for users.
 - Laravel Compatible API
 - Mobile Application Framework must be developed using “Flutter”

F.1.8 Mobile Application Development Training on Flutter Application Environment

- The training objective is to immerse PAGASA IT personnel in mobile

“Tracking the sky...helping the country”

application development, learn best practices on emerging technologies and gain new technical skill sets to enhance PAGASA Mobile application using Flutter application platform.

- Training modules must include at least with the following topics:
 - Introduction to Flutter
 - Getting Started with Flutter
 - Creating Flutter Apps from Scratch
 - Running and Testing Apps
 - Routing and Navigation
 - Databases and other Storages
 - Using Rest API, Parsing JSONs
 - Managing Flutter State
 - Programming Tips and Best Practices
 - Troubleshooting
 - Summary and Conclusion
- 7 personnel from PAGASA ICT (Face to Face)
- 5 Days Training (8 Hours per Day)
- Must be inclusive of meals and snacks.
- Preferred training site venue/location: Japan
- The training is intended for PAGASA IT managers in the area of:
 - Software Developers and Programmers
 - Other IT personnel involved in PAGASA Website Development
- Format of the Course
 - Interactive lecture and discussion.
 - Lots of exercises and practice.
 - Hands-on implementation in a live-lab environment.
- Training materials & certificates must be provided upon the completion of the course
- The winning bidder shall be responsible for covering all related expenses, such as, round trip airfare, transportation, lodging/accommodation, and allowable travel expenses per participant in accordance to the current UNDP-DSA rates

F.1.9 Mobile Application Development Devices

F.1.5.1 Mobile Phone Device Type A

Must provide one (1) unit with the following specifications:

- 6-core CPU with 2 performance and 4 efficiency cores or better
- 6.3-inch (diagonal) all-screen OLED display
- 2796-by-1290-pixel resolution at 460 ppi
- iOS 17 or better

F.1.5.2 Mobile Tablet Device Type A

Must provide one (1) unit with the following specifications:

- 6-core CPU or better
- 10.9-inch (diagonal) LED backlit Multi-Touch display with IPS technology
- 2360-by-1640-pixel resolution at 264 pixels per inch
- Operating System iPadOS 17 or better

F.1.5.3 Mobile Phone Device Type B

Must provide one (1) unit with the following specifications:

- 8-core CPU or better
- 168.3mm (6.6" full rectangle) / 163.7mm (6.4" rounded corners), 1080 x 2340 (FHD+), Super AMOLED, 16M
- Operating System - Android

F.1.5.4 Mobile Tablet Device Type B

Must provide one (1) unit with the following specifications:

- Chip - Octa-Core or better
- Display - 10.9", 2304 x 1440 (WUXGA+), TFT or better,
- Operating System – Android

F.1.9 Scope of Work

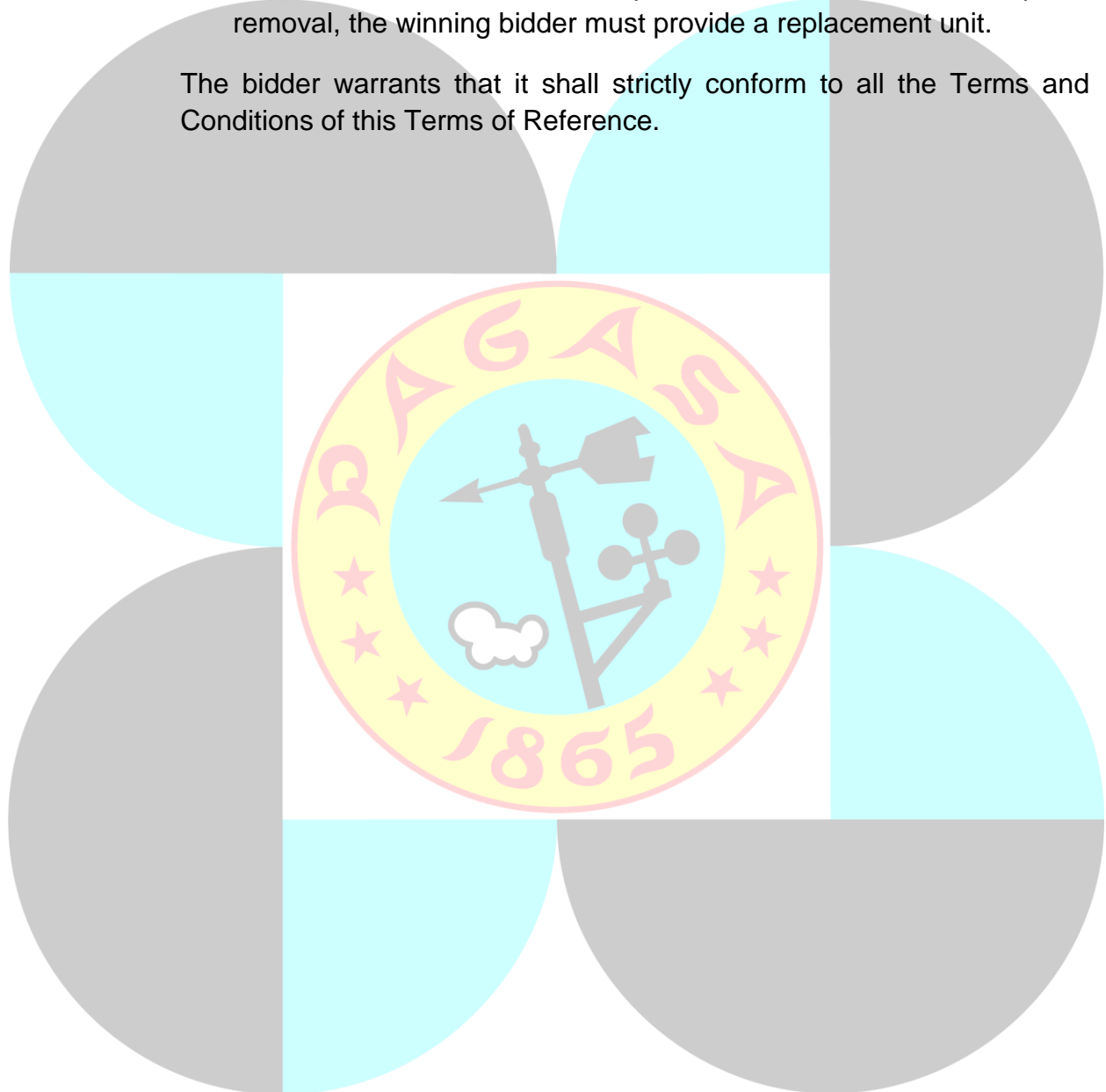
The scope of work covers the supply, delivery, installation, configuration, testing, training & commissioning of Integrated Firewall Solution and Mobile Application. The works and services to be performed under this contract shall essentially consist of, but not limited to, the following:

- Implementation
 - o Kick-off meeting must be conducted in coordination with the end-user in which the details of the project will be discussed. The schedule and venue will be advised by the end-user.
 - o Delivery, installation and configuration of Firewall appliance
 - o Installation, configuration and deployment of Application Security Testing environment and PAGASA Early Warning Mobile Application environment on existing PAGASA system environment.
 - o The firewall is required to operate continuously for a period of 7 days (168 hours) without experiencing any interruptions, malfunctions, or performance degradation.
- System training on software and hardware solutions
- 3 years hardware warranty, maintenance and support 24x7
- 1 year software warranty and subscription, including support available during workdays.
- System Acceptance

F.1.10 Service Level Agreement

- Technical support should be available via phone and onsite during the contract period.
- Defective equipment should be repaired within 48 hours, with parts replaced free of charge if found defective in materials or workmanship under normal and proper use.
- If the ICT hardware cannot be repaired due to difficulties and requires removal, the winning bidder must provide a replacement unit.

The bidder warrants that it shall strictly conform to all the Terms and Conditions of this Terms of Reference.



F.2.LOT B: SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION, COMMISSIONING & TRAINING OF RACK MOUNT SERVER

The winning bidder shall supply, deliver, install, configure, commission and train with the following at least minimum requirements:

F.2.1 Rack Mount Server Specification

The winning bidder must provide must provide one (1) unit of rack mount server with the following minimum specifications:

	Description	Quantity
Form Factor	2U Rack Mount	
Processor	6548Y+ (2.5GHz/32Cores/60MB/250W) CPU	2
Memory	64GB 2Rx4 DDR5-5600B RDIMM Memory Module	8
Storage 1	480GB 6G SATA 3.5in MU SSD	2
Storage 2	3.84TB 6G SATA 3.5in MU SSD	6
Storage 3	2.5" HDD TRAY IN 4TH GENERATION 3.5" HOT SWAP TRAY	8
Ports and Slots	12G SAS RAID Controller Module (Supporting 16 SAS Ports,8GB Cache, PCIe)	1
	2-Port 10GE Fiber Interface Ethernet Adapter (SFP+)	2
	TPM Module	1
Management	HDM Management System (with dedicated management port) iFIST/UniSystem	-
Standards	CE, UL, FCC, VCCI, CB, etc.	-
Security	Chassis Intrusion Detection TPM2.0 2FA for HDM Intel SGX2.0	-

F.2.2 UNIX / LINUX Network Administration and Security Training

- This training program helps the participants to configure multiple parts of a Linux system with the goal to optimize its functionality, reliability, performance and security.
- Training modules must at least include the following topics:
 - o Introduction to Network Services
 - o Organizing Networked Systems
 - o Network File Sharing Services
 - o Electronic Mail Services
 - o The HTTP Service
 - o Security Concerns and Policy
 - o Authentication Services
 - o System Monitoring
 - o Securing Networks
 - o Securing Services
 - o Securing Data
- At Least two (2) personnel from PAGASA ICT must be present
- Training Must be conducted in person (face to face)
- Must have at least Forty (40) Hours, Five (5)-days training workshop
- Meals, transportation allowance (if applicable), Training materials and certificates must be provided during the course duration.

F.2.3 WORKSTATION DEVICES

F.2.3.1 Workstation Laptop A

Must provide one (1) unit with the following specifications:

- Display – at least 15 to 16.9 inches
- Processor -16 cores or better
- Graphics - 6GB Dedicated VRAM or better
- Memory - 24GB RAM or better
- Storage - 1TB SSD or better
- Warranty – 1 Year Hardware Warranty

F.2.3.2 Workstation Laptop B

Must provide one (1) unit with the following specifications:

- Display – 16” or better
- Processor -16 cores or better
- Graphics - 12GB Dedicated VRAM or better
- Memory - 24GB RAM or better
- Storage - 1TB SSD or better
- Warranty - 1 Year Hardware Warranty

F.2.4 Scope of work

The scope of work covers the supply, delivery, installation, commissioning and configuration of Rack Mount Server. The works and services to be performed under this contract shall essentially consist of, but not limited to, the following:

- Delivery, installation, commissioning and configuration of Rack Mount Server
 - The server is required to operate continuously for a period of 7 days (168 hours) without experiencing any interruptions, malfunctions, or performance degradation.
- The winning bidder must assign at least two personnel to assist the PAGASA ICT in unboxing, and installation of hardware until the duration of inspection.
- System training on software and hardware solutions
- 3 years hardware warranty, maintenance and support
- System Acceptance

F.2.5 Service Level Agreement

- Technical support should be available via phone and onsite during the contract period
- Defective ICT equipment should be repaired/replaced within 48 hours, free of charge if found defective in materials or workmanship under normal and proper use.

G. SUMMARY OF ITEMS

LOT	ITEM
A	SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION, COMMISSIONING & TRAINING OF INTEGRATED FIREWALL SOLUTION AND SOFTWARE DEVELOPMENT <ul style="list-style-type: none"> • Integrated Firewall Solution • Application Security Testing Platform • Incident Handling Engineer Training (Introductory Course) • CCNA 1: Intro to Networks (ITN) Training • CCNA 2: Switching, Routing and Wireless Essentials (SRWE) Training • CCNA 3: Enterprise Networking, Security and Automation (ENSA) V7 • PAGASA Early Warning Mobile Application • Mobile Application Development Training on Flutter Application Environment • Mobile Phone Device Type A • Mobile Tablet Device Type A • Mobile Phone Device Type B • Mobile Tablet Device Type B
B	SUPPLY AND DELIVERY OF VARIOUS ICT TRAINING ON CYBER SECURITY, SYSTEM ADMINISTRATION AND DEVELOPMENT <ul style="list-style-type: none"> • Rack Mount Server • UNIX / LINUX Network Administration and Security Training • Workstation Laptop A • Workstation Laptop B

H. SITE ACCEPTANCE

- Two (2) supervisory personnel from the PAGASA ICT and Inspection Committee shall oversee and support the acceptance procedure, as well as the signing of the site acceptance certificate. This process, including the signing, will take place following the testing and commissioning of the deliverable items. Meals shall be provided by the winning bidder during the conduct of acceptance (breakfast, morning coffee break, lunch and afternoon coffee break).

I. GENERAL NOTE

- The winning bidder must provide a warranty certificate covering the ICT deliverable equipment.

- The winning bidder must have a certified true copy of a valid certificate of distributorship/dealership/reseller ship or professional partnership with the distributor/manufacturer of the brand for Integrated Firewall Solution, Application Security Testing Platform and Rack Mount Server.
- Quality assurance is expected from the winning bidders, such that any error or fault in any hardware, peripherals, preinstalled mandatory software and installation tools delivered during the implementation shall be acted upon, resolved, mitigated and/or replaced accordingly at no cost to the PAGASA. Likewise, upon final project acceptance, the winning bidder is required to after sales service and assurance that all equipment and installation are accurate, complete, operable, uncompromised and error-free during warranty.
- All components must be branded and should be factory installed with corresponding part numbers.

