REPUBLIC OF THE PHILIPPINES
Department of Science and Technology
Philippine Atmospheric, Geophysical and A
Services Administration (PAGASA)
Science Garden Complex, Agham Road, East Triangle, Diliman, Quezon City 1100

TECHNICAL SPECIFICATION FOR THE SUPPLY, DELIVERY, INSTALLATION, TESTING AND COMMISSIONING OF PAGASA WIRELESS LOCAL AREA NETWORK (WLAN)

This procurement intends to upgrade and rehabilitate in order to provide a holistic and best approach in the establishment of a secured and industry-standard compliant "Wireless Local Area Network (WLAN)" for PAGASA Central Office, WFFC and CAD buildings. The Approved Budget for Contract (ABC) is Nine Million Two Hundred Seventy Thousand Pesos (**P9,270,000.00**)

The following are the WLAN standard features that should be attained by the perspective bidders with their offered solutions:

- General Requirements
  - → Centralized WLAN architecture with "thin" Access Point and centralized controllers, and integrated network management
  - → Self-contained, integrated, overlay solution, not requiring upgrades or enhancements to existing routers and switches
  - → The same software, configurations and product functionality supported across all platforms in the product family proposed
  - → Wi-Fi Certified for Data
  - → Wireless solutions are 802.11 standards-based
  - → Controller must support not less than 100 AP
  - → Published Life-Cycle Announcements

- Security
  - → Support universal authentication
  - → MAC based authentication
  - → 802.1X based authentication
  - → Integrated Web-Based Authentication
  - → WPA2/AES link layer encryption
  - → Details are provided for key length, key exchange, key rotation, key Life Cycle Management, key crypto algorithms and message authentication algorithms used
  - → WEP link layer encryption
  - → LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-GTC authentication
  - → RADIUS support
  - → Ability to utilize RADIUS attributes to assign users or devices to specific roles/vlans.
  - → 802.1X supplicants
  - → User name and password authentication, as well as support for token based authentication.
  - → Facilitate process for non-IT staff to create temporary guest IDs and passwords to automatically expire/role provisioning
  - → Ability to customize the pre-authentication network access rights beyond DHCP response (e.g. to allow PCs and MACs to finish network scripts and network boot ups).
  - → API's for scripted control of these features from external system

→ 802.1X based guest access using a local database on the switch/controller that can be used to authenticate users.

The following are the breakdown and minimum specifications of the components of the required Wireless Local Area Network (WLAN):

- **ACCESS POINT (AP)** incl. license, update support, plug and mounting kits – **36 sets**
  - → Supports up to 2,166 Mbps per radio in the 5 GHz band (with 4SS/VHT80 or 2SS/VHT160 clients) and up to 800 Mbps in the 2.4 GHz band (with 4SS/VHT40 clients.
  - → Support for up to 256 associated client devices per radio and up to 16 BSSIDs per radio.
  - → Plenum rated with applicable certifications.
  - → One Auto-sensing link speed (100/1000/2500BASE-T) and MDI/MDX port for AP.
  - → One Auto-sensing 10/100/1000BASE-T Ethernet network interface (RJ-45) for AP.
  - → Eavesdropping on wireless user data and malicious attacks on Aps.
  - → Optionally support distributed Encryption/De-encryption (e.g. on AP's) without the need for specialized hardware with support mixed mode operations from a single switch/controller.
  - → Improve enterprise wide mobility by securing legacy devices with integrated client VPN and site-to-site VPN.
  - → Out of Band Management.
  - → Automatic updates of firmware and software on all APs without user intervention.
  - → Support discovery protocol from APs to find and sync with switch/controller, that works over routed and switched subnets and that does not require reconfiguration or features on routers or switches.
  - → All AP configuration and service delivery information centrally managed and maintained via the controller.
  - → Provides an easy to use (template based) mechanism to support configuration of different groups of APs – without requiring a separate management interface.
  - → Solution must have the ability to intelligently and dynamically load-balance devices without receiving a new association request from the device.
  - → Allow for automatic and manual RF radius adjustment.
  - → Provide support for RF coordination between Aps.
  - → Prevent data loss with adaptive RF management that provides the capability to pause channel scanning / adjust RF scanning intervals based on application and load presence.
  - → Load balancing across bands and steering of dual-band capable clients from 2.4GHz to 5GHz in order to improve network performance without the use of client specific configurations or software.
  - → High Density Coverage - the selected product must be able to support many thousands of devices in a single physical space.
  - → Traffic shaping capabilities to offer air-time fairness across different type of clients running different operating systems in order to prevent starvation of client throughput in particular in a dense wireless user population without the use of client specific configurations or software.
  - → Co-channel interference management in order to prevent adverse effects of operating multiple APs in the same channel while in close proximity.

- → Security enforcement for wireless users through the use of a role-based, stateful firewall that can be directly integrated with the roles defined within existing authentication servers.
- → Dynamic, stateful access rights into the network once authenticated based on source, destination, and/or ports.
- → Capability to ensure privacy protection by preventing firewall and IP spoofing attacks, and enforcing TCP handshake.
- → Access policies should provide for automatic capture of data and syslog of access rule triggers for audit and analysis.
- → Provide specific destinations, ports and IP protocol pass through option for captive portal networks.
- → Must support a plan to transition the current captive portal product to the proposed solution.
- → Packet-rate based bandwidth contract for individual guest users for increased control of guest traffic usage.
- → Provide application, user, and policy based QoS.
- → Prevent mis-use of QoS rules with deep packet inspection and WMM queue enforcement for user data.
- → Supports controller-managed mode.
- → Support 802.3af/at standard Power-over-Ethernet (PoE).
- → Support AP pre-configuration (before AP is installed).
- → Support out-of-the box, auto configuration across layer-2 and layer-3 networks.
- → "Hard configured" internal network information or certificates for authentication should not be hold at the AP unless stored in a trusted platform module (TPM) integrated into the AP.
- → Minimum of 8 SSIDs and BSSIDs available on each AP simultaneously without negatively impacting system performance.
- → Capable of multi-function services including: data access, intrusion detection, intrusion prevention, location tracking, and RF monitoring with no physical "touch" and no additional cost.
- → Real-time, fully integrated spectrum analyzer capabilities on the APs, that does not require dedicated sensors or separate operating system running on the AP radios.
- → Built-in Bluetooth Low-Energy (BLE) radio.
- → Advanced Cellular Coexistence (ACC). Minimizes interference from 3G/4G cellular networks, distributed antenna systems, and commercial small cell/femtocell equipment.
- → Supports multi-user MIMO (MU-MIMO) and 4 spatial Access Point streams (4SS)
- → Wi-Fi alliance 802.11a/b/g/n/ac.
- → 802.11ac wave 2 APs should be backward compatible to cat-5e and 802.3at power standards.
- → The AP must have AppRF technology leverages deep packet inspection to classify and block, prioritize, or limit bandwidth for thousands of applications in a range of categories.
- → The AP must minimize interference from 3G/4G cellular networks, distributed antenna systems and commercial small cell/femtocell equipment.
- → Enables location-based services with BLE-enabled mobile devices receiving signals from multiple Beacons at the same time.
- → The AP must support quality of service for unified communications applications - Supports priority handling and policy enforcement for unified communication apps, including Skype for Business with encrypted videoconferencing, voice, chat and desktop sharing.

- **ACCESS POINT CONTROLLER** incl. license, update and other support- **2 Sets**

  → The controller must be able to handle maximum 64 AP.
  → The controller must be capable of maximum 4,096 concurrent users.
  → The controller must have 1,024 concurrent GRE tunnels.
  → The controller must have 2,048 concurrent sessions.
  → The controller must have 8 Gbps firewall throughput.
  → The controller must support VLAN tagging with maximum of 4,094 VLANS.
  → The controller must have 8 dual personality ports (auto-negotiating 10/100/1000BASE-T) or Gigabit Ethernet ports (GBIC or SFP).
  → Use of industry standards-based (IEEE or IETF) tunneling protocols; specify standard that the tunneling mechanism is based on.
  → Centralized Encryption/De-encryption (e.g. on switch/controller in data center) to prevent wired.
  → Eavesdropping on wireless user data and malicious attacks on Aps.
  → Optionally support distributed Encryption/De-encryption (e.g. on AP's) without the need for specialized hardware with support mixed mode operations from a single switch/controller.
  → Improve enterprise wide mobility by securing legacy devices with integrated client VPN and site-to-site VPN.
  → Out of Band Management.
  → Automatic updates of firmware and software on all APs without user intervention.
  → Support discovery protocol from APs to find and sync with switch/controller, that works over routed and switched subnets and that does not require reconfiguration or features on routers or switches.
  → All AP configuration and service delivery information centrally managed and maintained via the controller.
  → Provides an easy to use (template based) mechanism to support configuration of different groups of APs – without requiring a separate management interface.
  → Solution must have the ability to intelligently and dynamically load-balance devices without receiving a new association request from the device.
  → Allow for automatic and manual RF radius adjustment.
  → Provide support for RF coordination between Aps.
  → Prevent data loss with adaptive RF management that provides the capability to pause channel scanning / adjust RF scanning intervals based on application and load presence.
  → Load balancing across bands and steering of dual-band capable clients from 2.4GHz to 5GHz in order to improve network performance without the use of client specific configurations or software.
  → High Density Coverage - the selected product must be able to support many thousands of devices in a single physical space.
  → Traffic shaping capabilities to offer air-time fairness across different type of clients running different operating systems in order to prevent starvation of client throughput in particular in a dense wireless user population without the use of client specific configurations or software.
  → Co-channel interference management in order to prevent adverse effects of operating multiple APs in the same channel while in close proximity.

- → Security enforcement for wireless users through the use of a role-based, stateful firewall that can be directly integrated with the roles defined within existing authentication servers.
- → Dynamic, stateful access rights into the network once authenticated based on source, destination, and/or ports.
- → Capability to ensure privacy protection by preventing firewall and IP spoofing attacks, and enforcing TCP handshake.
- → Access policies should provide for automatic capture of data and syslog of access rule triggers for audit and analysis.
- → Provide specific destinations, ports and IP protocol pass through option for captive portal networks.
- → Must support a plan to transition the current captive portal product to the proposed solution.
- → Packet-rate based bandwidth contract for individual guest users for increased control of guest traffic usage.
- → Provide application, user, and policy based QoS.
- → Prevent mis-use of QoS rules with deep packet inspection and WMM queue enforcement for user data.
- → Support advanced multicast features with multicast rate optimization, multi-channel use and IGMP snooping.
- → Packet Loss Prevention.
- → Traffic prioritization.
- → The system must support internal routing, bridging and spanning tree capabilities across its ports within the centralized switch/controller in order to enable ease of deployment and scalability.
- → An internal DHCP server for ease of deployment and scalability must be available and must be able to redistribute dynamically learned information.
- → Provide IPv6 support for the system and client devices.
- → Command line interface to control and manage all aspects of the system on the controller/switch.
- → Administrative rights partitioning - different admins have different rights.
- → Provide audit trail of administrative actions.

- **POE INJECTOR**
  - → AC 100-240 V
  - → 30 Watt
  - → Complies to IEEE 802.3at PoE standard and is backward compatible to IEEE802.3af.

- **FIVE (5) - YEAR SERVICE COVERAGE**
  - → 24/7 service for the period of 5 years starting from date of acceptance
  - → Level of service must be explicitly stated
  - → Covers services and change of equipment in case of unrepairable defects

SCOPE OF WORKS

1. Provision of access point and peripherals.
2. Wifi radius checking on all sites and AP location determination finalization
3. Mounting of access points
4. Provision of network power and signal
5. Configuration of AP
6. Configuration of AP to the AP controller
7. AP controller traffic shaping configuration
8. Sketching of WLAN network
9. Final testing and Commissioning of system

GENERAL NOTE:

All prospective bidder shall provide in their bid proposal the following documents:

- **WiFi coverage diagrams on all areas concerned as a result of a conducted survey.** The diagrams must explicitly show the particular RF signal strength on all areas covered by the project.
- **Certificate of site survey duly signed by the end user.**
- **This is a one brand solution, all main components must be coming from one brand.**
- **Proposed SLA for the 5 year service coverage.**