REPUBLIC OF THE PHILIPPINES

DEPARTMENT OF BUDGET AND MANAGEMENT

GENERAL SOLANO STREET, SAN MIGUEL, MANILA

SUPPLEMENTAL/BID BULLETIN (SBB) NO. 1

This SBB No. 1 dated December 11, 2018 for the Project, "Wireless Controller and Access Point Replacement," is issued to clarify, modify or amend items in the Bidding Documents. Accordingly, this shall form an integral part of said Documents.

<table>
<tr><th>PARTICULARS</th><th>CLARIFICATION/AMENDMENTS</th></tr>
<tr><td>

Section VI. Schedule of Requirements

Item	Description	Quantity	Delivery Schedule
1	WLAN Controller	1 unit	Sixty (60) calendar days from issuance of Notice to Proceed
2	Access Point (Branded and Brand New)	70 units	

Section VII. Technical Specifications

</td><td>

Section VI. Schedule of Requirements

Item	Description	Quantity	Delivery Schedule
1	WLAN Controller	~~1 unit~~ **2 UNITS**	~~Sixty (60)~~ **NINETY (90)** calendar days from issuance of Notice to Proceed
2	Access Point (Branded and Brand New)	70 units	

- Please see the attached Revised Section VI. Schedule of Requirements

Section VII. Technical Specifications

- Please see the attached Revised Section VII. Technical Specifications-ANNEX A

</td></tr>
</table>

Other matters:

- The "No Contact Rule" shall be strictly observed. Bidders are not allowed to call or talk to any member of the Bids and Awards Committee, Technical Working Group or Secretariat effective December 18, 2018 right after the opening of bids.

- For guidance and information of all concerned.

CLARITO ALEJANDRO D. MAGSINO
Assistant Secretary
Chairperson, DBM-BAC

Section VI. Schedule of Requirements

(Revised)

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

Item	Description	Quantity	Delivery Schedule
1	WLAN Controller	2 units	Ninety (90) calendar days from issuance of Notice to Proceed.
2	Access Point (Branded and Brand New)	70 units	

I hereby certify to comply and deliver all the above requirements.

_____	_____	_____
Name of Company/Bidder	**Signature over Printed Name of Representative**	**Date**

ANNEX A

Technical Specifications
(Revised)

1.0 Name of Project

Wireless Controller and Access Point Replacement

2.0 Objective

To replace the WLAN controller and access point of the enterprise wireless network of DBM.

3.0 Scope

The Project is a supply, installation, commissioning (*device testing and pre-configuration*), and alignment of the devices and security solutions to the DBM enterprise wireless network system. Implementation must be completed within 60 calendar days from issuance of Notice to Proceed.

The bidder must have the following Certified Professionals for the active devices & security solutions testing, configuration and network interoperability implementation:

- Manufacturer-Certified Network Professional;
- Manufacturer-Certified Network Associate; and
- Certified Network Security Administrator and/or Professional.

One-time payment shall be made upon completion of project implementation and submission of full documentation of the project components and functional requirements. A certificate of acceptance shall be issued by the DBM ICTSS.

All equipment should be covered by one (1) year service and hardware warranty under the following terms:

Defective parts/accessories replacement	Replacement of the defective parts/accessories, if not repaired beyond one (1) month from report, of the same or better brand, model feature, quality and functionalities at no additional cost to DBM.
Repair for equipment	Provide service unit for the equipment undergoing repair of at least the same brand, model features and functionalities or its equivalent within 4 hours from report at no additional cost to DBM.
Technical support	Provide/render 24x7 technical support service that can be delivered in a form of telephone call, electronic mail, or on-site support.

4.0 Specification

<u>Two (2) Units of Branded and Brand New WLAN Controller</u>

Features:

Digital Network Architecture (DNA) Software Defined Access (SD-Access) Wireless

- Enables network access in minutes for any user or device to any application without compromising on security.
- Enables policy-based automation for wired and wireless, automated provisioning of wired and wireless networks, group-based policy for users and connected devices.

DNA Analytics and Assurance

- Enables comprehensive network visibility. Capable to collect data from users, devices, and applications to proactively identify problems. Network analytics and automation to increase availability and deliver a better user experience.

Optimized to enable 802.11ac Wave 2 next-generation networks, supporting:

- 20-Gbps throughput
- 1500 access points
- 20,000 clients
- 4096 VLANs

Radio Frequency (RF) management

- Proactively identifies and mitigates signal interference for better performance.
- Provides both real-time and historical information about RF interference affecting network performance across controllers, through systemwide integration with Cisco CleanAir technology.

Multimode with indoor, outdoor mesh access points

- Versatile controller with support for centralized, distributed, and mesh deployments to be used at different places in the network, offering maximum flexibility for medium-sized campus, enterprise, and branch networks.
- Centralized control, management, and client troubleshooting.
- Seamless client access in the event of a WAN link failure (local data switching).
- Highly secure guest access.
- Efficient access point upgrade that optimizes the WAN link utilization.
- Supports corporate wireless service for mobile and remote workers with secure wired tunnels to indoor Cisco Aironet access points supporting OfficeExtend mode.

Comprehensive end-to-end security

- Offers Control and Provisioning of Wireless Access Points (CAPWAP)-compliant Datagram Transport Layer Security (DTLS) encryption on the control plane between access points and controllers across remote WAN links.
- Management frame protection detects malicious users and alerts network administrators.
- Rogue detection for Payment Card Industry (PCI) compliance.
- Rogue access point detection and detection of denial-of-service attacks.

Fault tolerance and high availability

- Subsecond access point and client failover for uninterrupted application availability.
- Redundant 1 Gigabit Ethernet/10 Gigabit Ethernet connectivity.
- Solid-state device-based storage - no moving parts.
- Redundant, hot-swappable power supply.
- Enhanced system uptime with fast system restarts.

Enterprise Wireless Mesh that allows access points to dynamically establish wireless connections without the need for a physical connection to the wired network.

WLAN express setup that simplified GUI wizard for quick setup and intuitive dashboards for monitoring and troubleshooting.

High-performance video stream technology that optimizes the delivery of video applications across the WLAN.

Mobility, security, and management for IPv6 and dual-stack clients

- Highly secure, reliable wireless connectivity and consistent end-user experience
- Increased network availability through proactive blocking of known threats.
- Equips administrators for IPv6 planning, troubleshooting, and client traceability.

Wired/Switching/Routing

- IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX specification, 1000BASE-T. 1000BASE-SX, 1000-BASE-LH, IEEE 802.1Q VLAN tagging, and IEEE 802.1AX Link Aggregation.

Wireless Specifications

- IEEE 802.11a, 802.11b, 802.11g, 802.11d, WMM/802.11e, 802.11h, 802.11n, 802.11k, 802.11r, 802.11u, 802.11w, 802.11ac Wave1 and Wave2

Data Request For Comments (RFC)

- RFC 768 UDP
- RFC 791 IP
- RFC 2460 IPv6
- RFC 792 ICMP
- RFC 793 TCP
- RFC 826 ARP
- RFC 1122 Requirements for Internet Hosts
- RFC 1519 CIDR RFC 1542 BOOTP
- RFC 2131 DHCP
- RFC 5415 CAPWAP Protocol Specification
- RFC 5416 CAPWAP Binding for 802.11

Security standards

- IEEE 802.11i (WPA2, RSN)
- RFC 1321 MD5 Message-Digest Algorithm
- RFC 1851 ESP Triple DES Transform
- RFC 2104 HMAC: Keyed Hashing for Message Authentication
- RFC 2246 TLS Protocol Version 1.0
- RFC 2401 Security Architecture for the Internet Protocol
- RFC 2403 HMAC-MD5-96 within ESP and AH
- RFC 2404 HMAC-SHA-1-96 within ESP and AH
- RFC 2405 ESP DES-CBC Cipher Algorithm with Explicit IV
- RFC 2407 Interpretation for ISAKMP
- RFC 2408 ISAKMP
- RFC 2409 IKE
- RFC 2451 ESP CBC-Mode Cipher Algorithms
- RFC 3280 Internet X.509 PKI Certificate and CRL Profile
- RFC 4347 Datagram Transport Layer Security
- RFC 5246 TLS Protocol Version 1.2

Encryption

- Wired Equivalent Privacy (WEP) and Temporal Key Integrity Protocol-Message Integrity Check (TKIP-MIC): RC4 40, 104 and 128 bits (both static and shared keys)
- Advanced Encryption Standard (AES): Cipher Block Chaining (CBC), Counter with CBC-MAC (CCM), Counter with Cipher Block Chaining Message Authentication Code Protocol (CCMP)
- Advanced Encryption Standard (AES): Cipher Block Chaining (CBC), Counter with CBC-MAC (CCM), Counter with Cipher Block Chaining Message Authentication Code Protocol (CCMP)
- Secure Sockets Layer (SSL) and Transport Layer Security (TLS): RC4 128-bit and RSA 1024-bit and 2048-bit
- DTLS: AES-CBC
- IPsec: DES-CBC, 3DES, AES-CBC
- 802.1AE MACsec encryption

Authentication, Authorization, and Accounting (AAA)

- IEEE 802.1X
- RFC 2548 Microsoft Vendor-Specific RADIUS Attributes
- RFC 2716 PPP EAP-TLS

- RFC 2865 RADIUS Authentication
- RFC 2866 RADIUS Accounting
- RFC 2867 RADIUS Tunnel Accounting
- RFC 2869 RADIUS Extensions
- RFC 3576 Dynamic Authorization Extensions to RADIUS
- RFC 5176 Dynamic Authorization Extensions to RADIUS
- RFC 3579 RADIUS Support for EAP
- RFC 3580 IEEE 802.1X RADIUS Guidelines
- RFC 3748 Extensible Authentication Protocol (EAP)
- Web-based authentication
- TACACS support for management users

Management

- Simple Network Management Protocol (SNMP) v1, v2c, v3
- RFC 1155 Management Information for TCP/IP-Based Internets
- RFC 1156 MIB
- RFC 1157 SNMP
- RFC 1213 SNMP MIB II
- RFC 1350 TFTP
- RFC 1643 Ethernet MIB
- RFC 2030 SNTP
- RFC 2616 HTTP
- RFC 2665 Ethernet-Like Interface Types MIB
- RFC 2674 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual Extensions
- RFC 2819 RMON MIB
- RFC 2863 Interfaces Group MIB
- RFC 3164 Syslog
- RFC 3414 User-Based Security Model (USM) for SNMPv3
- RFC 3418 MIB for SNMP
- RFC 3636 Definitions of Managed Objects for IEEE 802.3 MAUs
- Cisco private MIBs

Management Interfaces

- Web-based: HTTP/HTTPS
- Command-line interface: Secure Shell (SSH) Protocol, serial port

Interfaces and Indicators

- 2 x 10 Gigabit Ethernet interfaces
- Small Form-Factor Pluggable (SFP)/Small Form-Factor Pluggable Plus (SFP+) options (only Cisco SFP/SFP+s supported), including S-Class Optics.
- 1 x service port: 1 Gigabit Ethernet port (RJ-45)
- 1 x redundancy port: 1 Gigabit Ethernet port (RJ-45)
- 1 x Cisco Integrated Management Controller port: 10/100/1000 Ethernet
- 1 x console port: Serial port (RJ-45)
- LED indicators: Network Link, Diagnostics

Seventy (70) Units of Branded and Brand New Access Point

Features:

Flexible radio assignment that allows the access points to intelligently determine the operating mode of serving radios based on the RF environment. The access points can operate in the following modes:

- 2.4-GHz and 5-GHz mode: One radio will serve clients in 2.4-GHz mode, while the other serves clients in 5-GHz mode.
- Dual 5-GHz mode: Both radios inside the access point operate on the 5-GHz band, maximizing the benefits of 802.11ac Wave 2 and increasing client device capacity.

- Security Monitoring and 5-GHz mode, One radio will serve 5-GHz clients, while the other is scanning the full spectrum for wIPS attackers, CleanAir interferers, and rogue devices.

Dual 5-GHz radio support that enables both radios to operate in 5-GHz client serving mode, allowing an industry-leading 5.2 Gbps (2 x 2.6 Gbps) over-the-air speeds while increasing client capacity.

Smart antenna connector that provides advanced network design flexibility for high-density and large open-area environments such as auditoriums, libraries, cafeterias, and conference room, allowing two sets of antennas to be connected and active on a single access point.
Supporting channels up to 160 MHz wide, Dynamic Bandwidth Selection allows the access point to dynamically switch between 20-, 40-, 80-, and 160-MHz channels, depending on the RF channel conditions, providing the industry's best-performing wireless network.
Optimized access point roaming to ensure that client devices associate with the access point in their coverage range that offers the fastest data rate available.

Zero impact application visibility and control that uses dedicated hardware acceleration to improve the performance of line-speed applications such as Application Visibility and Control.

Auto link aggregation (LAG) allowing both Gigabit Ethernet interfaces to automatically LAG, increasing overall throughput to the access point.

ClientLink 4.0 technology to improve downlink performance to all mobile devices, including one-, two-, and three-spatial-stream devices on 802.11a/b/g/n/ac while improving battery life on mobile devices such as smartphones and tablets.

Multipole-Input and Multiple-Output (MIMO) equalization capabilities, which optimize uplink performance and reliability by reducing the impact of signal fade. 802.11n version 2.0, 802.11ac Wave1/Wave2 capabilities:

- 4x4 MIMO with three spatial streams
- Maximal Ratio Combining (MRC)
- 802.11n/802.11ag/802.11ac beamforming
- 20- /40-/80- /160-MHz channels
- PHY data rates up to 450 Mbps (40 MHz with 5 GHz)/1.3 Gbps (80 MHz in 5GHz/ 5.2 Gbps.
- Packet aggregation: A-MPDU (Tx/Rx), A-MSDU (Tx/Rx)
- 802.11 Dynamic Frequency Selection (DFS)
- Cyclic Shift Diversity (CSD) support

Integrated antenna, flexible radio (either 2.4 GHz or 5 GHz)

- 2.4 GHz, gain 4 dBi, internal antenna, omnidirectional in azimuth.
- 5 GHz, gain 6 dBi, internal directional antenna, elevation plane beamwidth 90°.
- Dedicated 5 GHz radio, gain 5 dBi, internal antenna, omnidirectional in azimuth

System memory

- 1024 MB DRAM
- 256 MB flash

Interfaces and Indicators

- 2x100/1000BASE-T autosensing (RJ-45)
- Management console port (RJ-45)
- USB 2.0 (enabled via future software)
- Status LED indicates boot loader status, association status, operating status, boot loader warnings, boot loader errors.

5.0 Confidentiality of Data

5.1 All project personnel of Bidder should be required to sign a non-disclosure agreement.

5.2 The DBM Enterprise Network System, its component, parts and all products, products samples and specifications, data, ideas, technology, and technical and non-technical materials, all or any which may be derived from any of the foregoing (all of which, individually and

collectively, referred to as "Proprietary Information") are confidential and proprietary to DBM.

5.3 The Bidder agrees to hold the Proprietary Information in strict confidence. Bidder furthermore agrees not to reproduce, translate or disclose the Proprietary Information to 3rd parties without prior written approval of the DBM.