Republic of the Philippines
CIVIL AVIATION AUTHORITY OF THE PHILIPPINES

BAGONG PILIPINAS

04 December 2023

BID BULLETIN NO. 3

I. Attention is hereby invited to the Bidders of the **"Supply, Delivery, Installation and Commissioning of IT Network Infrastructure at CAAP Various Airports including 1-Year Subscription of Internet Dedicated Access" (Bid No. 23-048-10).**

II. Please be informed of the following clarification/revision:

A. NEUTRALITY AND GENERIC SPECIFICATIONS

All items in the specifications and terms of reference are intended to be neutral and generic and must not favor an exclusive or single manufacturer. If terminologies are found to be brand exclusive, bidders are allowed and encouraged to propose an equivalent component/functionality that must be able to perform a comparable or better function to the listed item. Moreover, the proposed equivalent must be fully compatible, supports security, scalability, and seamless network operations with the existing network equipment, network security devices, and network management systems of the CAAP.

Bidders, including their partner-product manufacturer and the components proposed for the project must have no derogatory record or information on issues concerning cybersecurity and data security, both locally and internationally. In the interest of national security, the BAC reserves the right to disqualify any bid based on any well-grounded and reasonable belief that the components submitted by the bidders will compromise, endanger, or threaten the integrity of the CAAP IT Network Infrastructure.

B. QUERIES AND CLARIFICATIONS

ORIGINAL	REVISION/CLARIFICATION
3.1.1 the internet service provider must provide a certification that it uses its own domestic nationwide network and operates its own landing stations with at least 3 landing station facility must support IPV6, or its network platform is IPV6 ready and compliant	3.1.1 Changed to - The winning bidder shall provide its Internet Service Provider's certification that it uses its own domestic nationwide network and operates its own landing stations with at least 2 cable landing stations facility.
3.1.4 The internet service provider must have 30 peering connections to global internet service providers and content providers through a commercial and bilateral peering arrangements	3.1.4 Changed to - The internet service provider must have 15 peering connections to global internet service providers and content providers through a commercial and bilateral peering arrangement
3.1.6 The internet service provider must have five international internet points of presence and using redundant submarine cable systems to connect to its international nodes. Enumerate list of submarine routes	3.1.6 Changed to - The internet service provider must have at least two (2) international internet points of presence and using redundant submarine cable systems to connect to its international nodes.
3.1.8The Internet Service Provider must provide a certification that it's network platform is compliant to the latest MEF Carrier Ethernet (3.0) in all	3.1.8 The winning bidder shall provide its Internet Service Provider's certification that its network platform is compliant to the latest MEF Carrier Ethernet (2.0) in all Ethernet Service Types.

Ethernet Service Types. 3.1.9 The internet service provider	3.1.9 Deleted from the TOR
4.1.4 Tech Spec Specifications of Internet Connectivity 4.1.4.1 Must provide a dedicated, high-speed, diverse, reliable and managed connectivity to the Internet and guaranteed Internet bandwidth	The Type of Access – Fixed Bandwidth: - 200mbps: sites with CAAP Office only 1. Clark Int'l Airport (CAAP Office) 2. Mactan-Cebu Int'l Airport (CAAP Office) 3. Davao Int'l Airport (CAAP Office) - 400mbps: sites including CAAP Offices and other airport buildings and facilities 1. Laoag Intl Airport 2. Tuguegarao Airport 3. Pto. Princesa Airport 4. Bicol Intl Airport 5. Kalibo Intl Airport 6. Bacolod-Silay Airport 7. Panglao Airport 8. Tacloban Airport 9. Pagadian Airport 10. Zamboanga Intl Airport 11. Laguindingan Airport 12. Gen Santos Intl Airport Each site must include 4 usable IP
4.1.3.8.25 Item 5) Support access resource (destination IP/system) by NAT (NGAF IP address) or virtual IP 4.1.3.8.49 The vendor of the proposed solution must be certified with CMMI L5	4.1.3.8.25 Support access resource (destination IP system) by NAT (NGFW IP address) or virtual IP 4.1.3.8.49 Deleted
4.1.3.4.11 minimum flash storage of 32GB SDRAM 8GB Data buffer 32GB 4.1.3.4.12 minimum switching capacity 1.12 Tbps	4.1.3.4.11 changed to – minimum flash storage of at least 16 GB SDRAM at least 4GB Data buffer at least 16MB 4.1.3.4.12 Changed to minimum switching capacity of at least 900Gbps
4.1.3.5.5 minimum of 48 ports 10/100/100 base T RJ45 with POE 4.1.3.5.54 ARP poisoning detection 4.1.3.5.55 IP source filtering as a protective and effective mechanism against ARP attack	4.1.3.5.5 minimum of 48 ports 10/100/100 base T RJ45 with POE and 4X 10Ge SFP+ports 4.1.3.5.54 changed to- Dynamic ARP inspection 4.1.3.5.55 changed to- Dynamic ARP inspection
4.1.3.9.34 must be capable of up to 32 SSID	4.1.3.9.34 Changed to - Must be capable of at least 16 SSID
4.1.3.12: Must have a point-to-point radio to interconnect the buildings that are deemed necessary but not possible for wired connectivity.	Due to difference in distances of each building sites, the required specifications for the point-to-point radio shall be determined by the prospective bidder during the site inspection. Minimum requirement: dual band 2.4ghz/5.0Ghz, guaranteed bandwidth and not less than 400mbps upon installation and testing. License free frequencies accepted.

4.1.5 Specification of Wifi landing page with application to person or messaging capability 4.1.5 Wifi landing page should be part of the specification of the access points	CAAP will afford the winning bidder to propose the architecture and work flow on how the captive portal/Wifi landing page, subject to CAAP approval for implementation

TECHNICAL SPECIFICATIONS FOR 24 PORTS POE/NON-POE AND 8 PORTS POE ACCESS SWITCH

24 PORTS POE/NON-POE ACCESS SWITCH
The switch must support the following characteristics
Total RU: 1 RU maximum
Power Supply must be internal and integrated into the switch
SFP`s Hot Swap
Minimum of 24 ports 10/100/1000 Base T RJ45 with PoE+
Minimum of 2 SFP+ ports (1/10Gbps) for Uplink
Minimum of 2 1000BaseT/SFP combo ports
Equipment MUST be Fanless
Maximum Stack of 4 elements (Single Management IP)
Minimum switching capacity of 92Gbps
Minimum VFL (aggregated) of 40Gbps
Minimum Processing Capacity (Mpps): 68 Mpps
Operating Temperature: at least 0°C to 40°C
Humidity (operation): at least 5% to 90% non-condensing
PoE Budget of 180W
The switch must support the following Resiliency and high availability functionalities
IEEE protocol auto-discovery
Built-in CPU protection against malicious attacks
Split Virtual Chassis protection
The switch must support the following L3 protocols and features
Static routing for IPv4 and IPv6
Up to 64 IPv4 and 4 IPv6 static routes
Up to 32 IPv4 and 4 IPv6 interfaces
The switch must support the following layer-2 capabilities:
Up to at least 8k MAC Addresses
Up to at least 2000 VLANs
Up to 1.5k total system policies
Latency: < 4 µs
Max Frame: 9216 bytes (jumbo)
The switch must support the following features
Multicast Listener Discovery (MLD) v1/v2 snooping
Autosensing IEEE 802.1X multiclient, multi-VLAN support
Web based authentication (captive portal): a customizable web portal residing on the switch
Dynamically provide pre-defined policy configuration to authenticated clients — VLAN, ACL, BW
Secure Shell (SSH) with public key infrastructure (PKI) support
Centralized Remote Access Dial- In User Service (RADIUS) and Lightweight Directory Access Protocol (LDAP) administrator authentication
Centralized RADIUS for device authentication and network access control authorization
Learned Port Security (LPS) or MAC address lockdown
Access Control Lists (ACLs); flow-based filtering in hardware (Layer 1 to Layer 4)

DHCP Snooping, DHCP IP and Address Resolution Protocol (ARP) spoof protection
ARP poisoning detection
IP Source Filtering as a protective and effective mechanism against ARP attacks
The switch must support Quality of Service (QoS) features
Intuitive CLI in a scriptable BASH environment via console, Telnet, or Secure Shell (SSH) v2 over IPv4/IPv6
Powerful WebView Graphical Web Interface via HTTP and HTTPS over IPv4/ IPv6+
File upload using USB, TFTP, FTP, SFTP, or SCP using IPv4/IPv6
Human-readable ASCII-based configuration files for off-line editing, bulk configuration, and out-of-the-box auto-provisioning
Multiple microcode image support with fallback recovery
Dynamic Host Configuration Protocol (DHCP) relay for IPv4/IPv6
DHCPv4 and DHCPv6 server
The switch must compatible with CAAP existing network switches and network management software
8 PORTS POE ACCESS SWITCH
The switch must support the following characteristics
Total RU: 1 RU maximum
Power Supply must be internal and integrated into the switch
SFP`s Hot Swap
Minimum of 8 ports 10/100/1000 Base T RJ45 with PoE+
The above minimum ports quantity cannot be combo ports. All ports must be available in the switch, and at the same time
Equipment must be fanless
Maximum Stack of 4 elements (Single Management IP)
Minimum switching capacity of 40Gbps
Minimum Processing Capacity (Mpps): 17.9 Mpps
Operating Temperature: at least 0°C to 40°C
Humidity (operation): at least 5% to 90% non-condensing
PoE Budget of 120W
The switch must support the following Resiliency and high availability functionalities
IEEE protocol auto-discovery
Built-in CPU protection against malicious attacks
Split Virtual Chassis protection
The switch must support the following L3 protocols and features
Static routing for IPv4 and IPv6
Up to 64 IPv4 and 4 IPv6 static routes
Up to 32 IPv4 and 4 IPv6 interfaces
The switch must support the following layer-2 capabilities:
Up to at least 800 MAC Addresses
Up to at least 2000 VLANs
Up to 1.5k total system policies
Latency: < 4 µs
Max Frame: 9216 bytes (jumbo)
The switch must support the following features:
IGMPv1/v2/v3 snooping to optimize multicast traffic
Multicast Listener Discovery (MLD) v1/v2 snooping
Autosensing IEEE 802.1X multiclient, multi-VLAN support
MAC-based authentication for non-IEEE 802.1X hosts
Web based authentication (captive portal): a customizable web portal residing on the switch

Dynamically provide pre-defined policy configuration to authenticated clients — VLAN, ACL, BW
Secure Shell (SSH) with public key infrastructure (PKI) support
Centralized Remote Access Dial- In User Service (RADIUS) and Lightweight Directory Access Protocol (LDAP) administrator authentication
Centralized RADIUS for device authentication and network access control authorization
Learned Port Security (LPS) or MAC address lockdown
Access Control Lists (ACLs); flow based filtering in hardware (Layer 1 to Layer 4)
DHCP Snooping, DHCP IP and Address Resolution Protocol (ARP) spoof protection
ARP poisoning detection
IP Source Filtering as a protective and effective mechanism against ARP attacks
The switch must support Quality of Service (QoS) features
Intuitive CLI in a scriptable BASH environment via console, Telnet, or Secure Shell (SSH) v2 over IPv4/IPv6
Powerful WebView Graphical Web Interface via HTTP and HTTPS over IPv4/ IPv6+
File upload using USB, TFTP, FTP, SFTP, or SCP using IPv4/IPv6
Human-readable ASCII-based configuration files for off-line editing, bulk configuration, and out-of-the-box auto-provisioning
Dynamic Host Configuration Protocol (DHCP) relay for IPv4/IPv6
DHCPv4 and DHCPv6 server
The switch must be compatible with CAAP existing network switches and network management software

C. Bids must be duly received by the BAC Secretariat through manual submission at the office address indicated below on or before **13 December 2023 @ 9:30 AM**. Late bids shall not be accepted.

Address:

Bids and Awards Committee (BAC) Office
Civil Aviation Authority of the Philippines
MIA Road corner Ninoy Aquino Avenue1300
Pasay City, Metro Manila

For the information and guidance of all concerned.

ATTY. DANJUN G. LUCAS
Chairperson
Bids and Awards Committee - Bravo