Office of the President
of the Philippines
Malacañang

BID BULLETIN

Pursuant to the Invitation to Bid published last 13 September 2018 in Business Mirror, in PhilGEPS, OP-website and three conspicuous places regarding the project – **One (1) Lot Supply and Delivery of Network Switches and Fifteen (15) Other Line Items for the Mabini Hall Bldg. Structured Cabling Project.** with Purchase Request (PR) No. 18-08-0936 please be informed of the following changes resolved by the Bids and Awards Committee (BAC) during the Pre-bid Conference held on 20 September 2018, 1:30PM, at the OP-BAC Bidding Room, Mezzanine Flr., Mabini Hall Building, Malacañang, Manila and noted the recommendation of the End-user as to the amendments/changes to the Bidding Documents, as follows:

1. Technical Specifications:

FROM	TO
10GBASE-SR SFP Module	10GBASE-LRM SFP Module

2. Terms of Reference:

I. OBJECTIVE/PURPOSE

The Project seeks to install/layout of new structured cabling at Mabini Hall Building and to replace the outdated network switches and upgrade the Office of the President's (OP) Network Infrastructure System thru the introduction of appropriate network structure/configuration and greater capacity devices, among others.

Specifically, this Project aims to provide the following:

- Reliable interconnection from Mabini Hall to 8888 Citizens' Complaint Center, Bahay Ugnayan (Presidential Complaint Center), Engineering Office, Kalayaan, Malacañang Palace, New Executive Building and Asset Management Office;
- Structured Cabling system will support multiple hardware uses and be suitable for today's needs and those of the future.
- Provides efficient transmission/receive/process of data and voice messages;
- Caters and regulate the flow of traffic within the network system;
- Secured sensitive data information;
- Increase available network bandwidth and performance;
- Ensures high availability of telecoms and network services; and
- Redundancy and/or back-up support for continues flow of ICT operations.

Project Overview and Description:

One of the main purpose of this Project is to connect various computer network devices at different sites and manage the flow and transmission of information/data across the network system of the entire Office. Per our existing network setup, these switches were separately installed at various locations of Mabini Hall Building, NEB, and Palace.

The newly advance technology of network switches will provide intent-based networking solutions and services that turn network traffic data into actionable insights; manage the unprecedented scale of connected devices and services; also provides granular insight into end-users, the devices they use, and the applications they access.

Thru this device (network switch), with updated software applications and proper configuration, the accounted traffic flow of data and voice services will further improve our network performance.

And finally, with network virtualization, the new network switches further provide network security system with solutions designed to interoperate and provide multilayered protection; and engage real-time data to secure access, provide intelligence, and sense suspicious activity even in encrypted traffic.

Proposed layout and schematic design of network switches is hereto attached.

II. TECHNICAL REQUIREMENTS

ACCESS LAYER

The access layer of the proposed network consists of

- access switches

Access switches shall meet the minimum functions:

- Must have 24 Gigabit Ethernet ports with line-rate forwarding performance
- Must consist of 2 10G SFP+ uplinks
- Must support stacking of up to 8 switches with 80 Gbps of stack throughput (optional)
- Must have Reduced power consumption and advanced energy management features
- Must consist of USB and Ethernet management interfaces for simplified operations
- Must have Application visibility and capacity planning with integrated Full (Flexiable) NetFlow and NetFlow-Lite
- Must be able to identify, classify and control of trusted internal network traffic through Domain Name System as an Authoritative Source (DNS-AS)

Network Security

- Must have MAC-based VLAN assignment
- Must have Comprehensive 802.1X Features
- Must have IPv6 First-Hop Security
- Must have Device Sensor and Device Classifier
- Must have features including Port Security, Dynamic ARP Inspection, and IP Source Guard.
- Must have private VLAN edge to provide security and isolation between switch ports, which helps ensure that users cannot snoop on other users' traffic
- Must have Unicast Reverse Path Forwarding (uRPF)
- Must have Multidomain Authentication
- Must have Access Control Lists (ACLs) for IPv6 and IPv4 for security and QoS
- Must have Secure Shell (SSH) Protocol, Kerberos, and Simple Network Management Protocol Version 3 (SNMPv3)
- Must have Switched Port Analyzer (SPAN)
- Must have TACACS+ and RADIUS authentication
- Must have MAC Address Notification
- Multilevel security on console access

- Must have Bridge protocol data unit (BPDU) Guard which shuts down Spanning Tree Port Fast-enabled interfaces when BPDUs are received to avoid accidental topology loops.
- Must have Spanning Tree Root Guard (STRG)
- Must have IGMP filtering
- Must support Dynamic VLAN assignment

Redundancy and Resiliency

- Must be able to provide Cross-stack EtherChannel
- Must be able to provide link redundancy with convergence time less than 100 milliseconds
- Must be able to provide IEEE 802.1s/w Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP)
- Must support Per-VLAN Rapid Spanning Tree (PVRST+)
- Must support Switch-port auto-recovery

Enhanced Quality of Service

- Must support up to eight egress queues per port and strict priority queuing
- Must support SRR and WTD
- Must have Flow-based rate limiting and supports up to 256 aggregate or individual policers per port
- Must support 802.1p class of service (CoS) and Differentiated Services Code Point (DSCP) classification, with marking and reclassification on a per-packet basis by source and destination IP address, MAC address, or Layer 4 TCP/UDP port number.
- Must have Cross-stack QoS

Operational Features

Must be able to consist of the following features:

- Must support DHCP
- Must support Stacking master configuration management
- Must support autonegotiation
- Must support DTP
- Must support LACP.
- Must support Automatic MDIX
- Must support UDLD
- Must support SDM
- Must support Local Proxy ARP
- Must support VLAN1 minimization
- Must support IGMP Snooping for IPv4 and IPv6 MLD v1 and v2
- Must support MVR
- Per-port broadcast, multicast, and unicast storm control

Application Visibility and Control

- Must have Flexible NetFlow which allows optimization of the network infrastructure, reducing operation costs, and improving capacity planning and security incident detection with increased flexibility and scalability
- Must have Domain Name System as an Authoritative Source (DNS-AS)

Network Management

- Must provide an extensive library of easy-to-use features to automate the initial and day-to-day management of your network
- Must be able to integrate hardware and software platform expertise and operational experience into a powerful set of workflow-driven configuration, monitoring, troubleshooting, reporting, and administrative tools

Power Management

- Must have Switch Hibernation Mode (SHM)
- Must support IEEE 802.3az EEE (Energy Efficient Ethernet)

III. SCOPE OF WORKS AND SERVICES

- Termination and Full Configuration of network switches
- All other components for supply only

A. WORK SCHEDULE

Working period shall be eight (8) hours a day from 8:00 AM to 5:00 PM, Monday to Friday, excluding legal and special holidays.

B. PAYMENT SCHEDULE

The payment for the maintenance services shall be thirty (30) days upon submission of the following:

- Billing Invoice
- Delivery Receipts of Materials
- As Built Plans
- Test Results
- Certificate of Work Acceptance

C. OTHER CONSIDERATIONS

ELIGIBILITY OF BIDDER

The Project Contractor must have the following classifications:

1. Must be certified reseller, installer, and/or partner of products being offered.
2. Minimum of ten (10) years in IT Business.
3. Must have at least five (5) previous contracts with government agency.

IV. DELIVERY/IMPLEMENTATION OF SERVICES

This project shall be completed for a period of forty-five (45) working days from the effectivity date of Notice to Proceed, **EXCLUDING** the necessary security clearance to be issued by the Presidential Security Group Command, Office of the President.

V. WARRANTY REQUIREMENT

The supplier shall provide maintenance service level agreement which includes twelve (12) months warranty on system parts & labor including on-site support upon acceptance of delivery of the hardware; service calls, repair or replace faulty items without charge.

VI. TRAINING REQUIREMENTS

Supplier shall provide the necessary training for the end-user's management and operation of the system upon completion of the Project.

Please be guided accordingly.

Atty. RYAN ALVIN R. ACOSTA
Chairman, OP – Bids and Awards Committee

26 September 2018

GMB/LOS/
OP-BAC