BIDS AND AWARDS COMMITTEE
2330 Roxas Boulevard, Pasay City
Tel. Nos. 834-4823; Fax No. 831-9584
Email: bac.secretariat@dfa.gov.ph

**SUPPLEMENTAL / BID BULLETIN No. 1**

| | | |
|---|---|---|
| Project | : | Procurement of Advance Malware Protection, Database Security and Application Security Solutions |
| Reference No. | : | PB-GS-06-2019 |
| ABC | : | PhP 10,000,000.00 |
| Date | : | 7 June 2019 |

---

This supplemental/bid bulletin is issued to provide information to the prospective proponents/bidders on the following changes to the Bidding Documents:

**I. Technical Specifications (Section VII) –** The Technical Specifications (Section VII) of the Bidding Documents is superseded by ANNEX A of this Supplemental/Bid Bulletin No. 1 after considering inputs from End-User, BAC Members and prospective bidders.

The Bidding Documents is amended accordingly.

For the information and guidance of all concerned.

**(Sgd.)**
**GENEROSO D.G. CALONGE**
Alternate BAC Chairperson

# TECHNICAL SPECIFICATIONS

**PROCUREMENT OF ADVANCE MALWARE PROTECTION, DATABASE SECURITY AND APPLICATION SECURITY SOLUTIONS**

| | | |
|---|---|---|
| I. | **BACKGROUND**<br><br>The Department of Foreign Affairs has already completed Phase 1 of the Secured Communications Network and now intends to proceed to Phase 2 to establish the secured network connectivity of all Foreign Service Posts (FSPs) and the DFA Main Building and DFA Aseana through the installation of Advance Malware Protection, Database Security and Application Security Solutions. | |
| II. | **OBJECTIVE**<br><br>Ensures that all FSPs establish a secured network connectivity and are protected from various cyber-attack and threats through a combined firewall, gateway anti-virus, and intrusion detection, accidental exposure of confidential information and prevention capabilities under a single solution. | |
| III. | **SCOPE OF WORK** | **Statement of Compliance** |
| | **A. CONTRACTOR RESPONSIBILITY** | |
| | 1. The Contractor shall supply and deliver to the DFA Main Building, a solution composed of appliances with three-year licenses. | |
| | 2. The Contractor shall provide technical/customer support for their software, during office hours five (5) days a week, excluding holidays. The Contractor shall guarantee 4-hour response and 6-hour resolution time during the warranty period.<br><br>A single point of contact shall be assigned to the Department for all technical issues and inquiries. | |
| | **B. SOLUTION REQUIREMENTS** | |
| | The Solution shall be composed of the following which are compatible with the existing solutions of the Department:<br><br>**Advance Malware Protection (AMP)**<br><br>**a. Cisco Meraki MX 84 (35 units)**<br>i. Stateful firewall throughput: 500Mbps<br>ii. Recommended maximum clients: 200<br>iii. Interfaces: 2x GbE RJ45 ports + 8x GbE RJ45 + 2xGbE (SFP)<br>iv. USB for 3G/4G failover<br><br>**b. Cisco Meraki MX 68 (15 units)**<br>i. Stateful firewall throughput: 450Mbps<br>ii. Recommended maximum clients: 50<br>iii. Interfaces: 2x GbE RJ45 ports + 10x GbE RJ45<br>iv. USB for 3G/4G failover | |
| | **Supervisor Engine Module for Catalyst 9407 – Sup1XL**<br>i. Centralized wired capacity of up to 1.44Tbps<br>ii. Per-slot switching capacity of 120Gbps<br>iii. Total number of IPv4 routing entries of up to 144,000 | |
| | **Access Switch Requirements** | |

| | | |
|---|---|---|
| | **a. Cisco Catalyst 9300 (1 unit)**<br>I. Shall have 1 x 24-ports of 10/100/1000 with 4 x 1G uplink<br>II. Shall have DNA advantage licenses<br>III. Shall have Solution Support Services<br><br>~~**b. Cisco Catalyst 9200 (1 unit)**~~<br>~~I. Shall have 1 x 24-ports of 10/100/1000 with 4 x 1G uplink~~<br>~~II. Shall have DNA advantage licenses~~<br>~~III. Shall have Solution Support Services~~<br><br>**c. Cisco Catalyst 3560CX-12TC-S ~~(6 units)~~ 4 units**<br>I. Shall have at least 1 x 12-ports of 10/100/1000<br>II. Shall have DNA advantage licenses<br><br>**d. CS-KIT-K9 Cisco Room Kit**<br>I. Integrated Microphone<br>II. Speakers<br>III. Touch 10 | |
| | **Database Security and Application Security** | |
| | **Technical Specifications** | |
| | a) Endpoint agents for 1500 users<br><br>b) Endpoint agent includes sophisticated tamper protection features that prevent an unauthorized end-user from disabling the endpoint agent. User with local or domain administrative permissions can configure an optional password to prevent unauthorized uninstallation of the agent.<br><br>c) Built-in template which conforms with the Philippine Data Privacy Act. Human-centric data-loss-protection approach with built-in incident risk ranking for behavioral analytics.<br><br>d) Endpoints that can monitor and block file uploads and file sync activity to both personal and enterprise cloud storage solutions. This is achieved both by monitoring application file access by cloud sync client software and by monitoring uploads to cloud sync web sites via web browsers (including Firefox and Chrome).<br><br>e) Endpoint provides capability to detect and include removable device data and allow search/filter incidents accordingly.<br><br>f) The policy engine, policies, and fingerprinted data are all resident on the data loss protection Endpoint. This means that policy will be applied whether on or off network.<br><br>g) Endpoint provides a simple Windows Server-based solution that enables managed endpoints to automatically update to a new version of the endpoint agent when it is available for data loss prevention, behavioral monitoring and vulnerability protection.<br><br>**h) On premise servers** | |

| | | |
|---|---|---|
| IV. | **CONTRACTOR QUALIFICATION** | |
| | 1. The Contractor must have at least five (5) years of experience in the supply, delivery, installation, testing, and commissioning of network installation and cabling services including systems integration. | |
| | 2. The Contractor shall be at least Certified ~~**Premier**~~ Partner of the brand being offered for at least five (5) years. | |
| | 3.The contractor shall provide three (3) technical engineers who must be directly employed by the contractor for at least one (1) year by the time of the project implementation. | |
| | 4. The Contractor shall submit a certification issued by the manufacturer's local office or its regional hub/distributor stating the following:<br><br>a. Endorsement of the Contractor to bid, sell/resell, support, and maintain the product being offered;<br>b. that all equipment is brand new and up to date;<br>c. that the Contractor is qualified to provide after sales service and parts for all the required equipment, accessories, and software; and<br>d. that the Contractor's single point of contact for technical support is qualified to support the Solution. | |
| | 5. The Contractor shall certify that it shall provide after sales service and parts for all the required equipment, accessories, and software included in this project for the next five (5) years commencing from the date of final acceptance by the Department.<br><br>The certificate shall include the Contractor's single point of contact, office address and official contact details. | |
| | 6. ~~The Contractor shall provide free CCNA-Security training and certification exam to five (5) technical personnel of the OAMSS-ITCRD on the installation, configuration, management and maintenance of the solution.~~<br>**The Contractor shall provide trainings and certification exam for the following:**<br>**a. Introduction to Cybersecurity and Cybersecurity Essentials for three (3) technical personnel of OAMSS-ITCRD**<br>**b. Certified Information Systems Manager for two (2) technical personnel of OAMSS-ITCRD** | |
| V. | **WARRANTY** | |
| | The Contractor shall provide 3-year warranty on parts and services commencing after full delivery of the Solution. | |
| VI. | **CONFIDENTIALITY CLAUSE** | |
| | 1. The Contractor shall ensure that each of its personnel assigned to provide support service executes and signs a Non-Disclosure Agreement which is to be submitted to the Department prior to commencement of the service.<br><br>2. The Contractor shall not disclose any confidential information accessed through the use of its services in relation to the official functions or operations of the Department without prior written consent from the latter. | |

| | | |
|---|---|---|
| | 3. The Contractor shall immediately inform the Department of breaches, attacks, or other forms of cyber threats/activities that may contribute to disclosure of any confidential information.<br><br>4. Failure to comply with the confidentiality clause shall be subject to penalties as provided in Republic Act No. 10173 – Data Privacy Act of 2012 and all other relevant rules and regulations. | |
| VII. | **DELIVERY AND PAYMENT** | |
| | 1. The Contractor shall deliver the Advance Malware Protection, Database Security and Application Security Solutions within thirty (30) calendar days upon receipt of Notice to Proceed (NTP);<br><br>2. The Contractor shall be paid within thirty (30) working days upon full delivery and submission of the sales invoice with complete supporting documents through List of Due and Demandable Accounts Payable (LDDAP); and<br><br>3. All payments shall be inclusive of all applicable taxes and other lawful charges. | |

**Note:**

Bidder must state compliance to each of the provisions in the Terms of Reference/Technical Specifications, as well as to the Schedule to Requirements. The **STATEMENT OF COMPLIANCE** must be signed by the authorized representative of the Bidder, with proof of authority to sign and submit the bid for and in behalf of the Bidder concerned. If the Bidder is a joint venture, the representative must have authority to sign for and in behalf of the partners to the joint venture. All documentary requirements should be submitted on or before the deadline for the submission of bids.

Bidders must state here either "Comply" or "Not Comply" against each of the individual parameters of each Specification stating the corresponding performance parameter of the equipment offered. Statements of "Comply" or "Not Comply" must be supported by evidence in a Bidders Bid and cross-referenced to that evidence. Evidence shall be in the form of a manufacturer's un-amended sales literature, unconditional statements of specification and compliance issued by the manufacturer, samples, independent test data etc., as appropriate. A statement that is not supported by evidence is subsequently found to be contradicted by the evidence presented will render the Bid under evaluation liable for rejection. A statement either in the Bidders statement of compliance or the supporting evidence that is found to be false either during Bid evaluation, post-qualification or the execution of the Contract may be regarded as fraudulent and render the Bidder or supplier liable for prosecution subject to the provisions of **ITB** Clause 3.1 (a)(ii) and/or **GCC** Clause 2.1 (a)(ii)

Conformé:

[Signature/s]
[Name of Bidder's Authorized Representative/s]
[Position]
[Date]