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. 2

Project	:	Procurement of Firewall/ Unified Threat Management Appliance (Secondary Cybersecurity Solution)
Reference No.	:	PB-GS-07-2016
ABC	:	PhP 13,500,000.00
Date	:	18 August 2017

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

ANNEX A of the Supplemental/Bid Bulletin No. 1 is superseded by **ANNEX A** of this Supplemental/Bid Bulletin No. 2.

The Bidding Documents is amended accordingly.

For the information and guidance of all concerned.

(Sgd.)
MARIA TERESA C. LEPATAN
BAC Chairperson

ANNEX A
Technical Specifications

FIREWALL/ UNIFIED THREAT MANAGEMENT APPLIANCE
(SECONDARY CYBERSECURITY SOLUTION)

I.	**BACKGROUND** The Department of Foreign Affairs (DFA) is the primary government agency implementing the Philippines' foreign policy. In working for the country's best interests in international relations, as well as providing services and protection for Filipinos abroad, the DFA maintains more than eighty-five embassies and consulate offices abroad (Foreign Service Posts / FSPs), twenty-one regional consular offices (RCOs) and several passport satellite offices (SOs) in the Philippines. The DFA Home Office serves as the central hub for administrative oversight and management of its Foreign Service Posts and regional offices, all of which rely on data, voice and software applications in order to perform its day-to-day activities, interacting with public clients as well as various inter-office transactions among its nearly 3,000 personnel.		
II.	**OBJECTIVE** The Department of Foreign Affairs requires technical equipment to support the interconnectivity between its various local and foreign offices, enabling various network services, telephony, current database applications and future information systems to be made available to remote sites and roaming users. To meet this target of providing security, site-to-site integration and connectivity, while ensuring protection from network intrusion, cyber attacks, malware, application-level strikes, backdoor threats, Trojans, and other internet-borne threats, the DFA seeks to acquire a comprehensive network security multifunction firewall/unified threat management package. It should meet its present and future needs within the approved budget of Thirteen Million Five Hundred Thousand Pesos (PhP 13,500,000.00) -- equipment, installation, training and all necessary licensing fees, and lawful taxes included.		
III.	**SCOPE OF WORK**		**Statement of Compliance**
	EQUIPMENT TYPE		
	Target Deployment	**Quantity**	
	Large enterprise / central office requiring high performance features to support approximately 1,500 host machines, 100 simultaneous site-to-site VPN connections, more than 200 roaming VPN clients.	**2**	
	Medium-size distributed office / branch office of about 500 host machines, 50 simultaneous site-to-site VPN connections, 50 roaming VPN clients	**6**	

	Stand-alone distributed offices of less than 100 host machines	**46**	
	TOTAL	**54**	
	CONTRACTOR RESPONSIBILITY		
	1. The Contractor shall supply, deliver, install and configure the FIREWALL APPLIANCE / UNIFIED THREAT MANAGEMENT SYSTEM at DFA Head Office and Office of Consular Affairs.		
	2. The FIREWALL APPLIANCE / UNIFIED THREAT MANAGEMENT SYSTEM shall be composed of licenses and appliances and shall be distributed as follows: a) DFA Main Office – two (2) units and 2 licenses b) OCA-ASEANA – two (2) units and 2 licenses c) FSPs – fifty (50) units and 50 licenses		
	3. The Contractor shall provide training to ten (10) technical personnel of the DFA specially on installation configuration, management and maintenance of the FIREWALL APPLIANCE / UNIFIED THREAT MANAGEMENT SYSTEM		
	4. The Contractor shall provide 24x7 technical/customer support, four (4) hours response and six (6) hours resolution time during the warranty period.		
	5. A single point contact shall be assigned to the DFA for all the technical inquiries/issues.		
	Firewall Appliance / Unified Threat Management System Requirements		
	6. **Hardware requirements for Firewall/UTM Appliance (2 units)** a) Stateful firewall throughput: 1Gbps b) Clients: At least 2000 c) Interfaces: 12x GbE (RJ45) + 8x GbE (SFP included) d) At least 3G wireless failover e) Firewall throughput in pass-through mode: 1 Gbps f) Firewall throughput, all security features enabled :1 Gbps		
	7. **Hardware requirements for Firewall/UTM Appliance (6 units)** a) Stateful firewall throughput: 750Mbps b) Clients: at least 500 c) Interfaces: 9x GbE + 2x GbE (SFP included) d) At least 3G wireless failover e) Firewall throughput in pass-through mode: 750 Mbps f) Firewall throughput, all security features enabled :650 Mbps		

	8. **Hardware requirements for Firewall/UTM Appliance (46 units)** a) Stateful firewall throughput: 500Mbps b) Clients: at least 200 c) Interfaces: 9x GbE ports + 2x GbE (SFP included) d) At least 3G wireless failover e) Firewall throughput in pass through mode: 500 Mbps f) Firewall throughput, all security features enabled: 320 Mbps	
	9. **Cloud-based centralized management** a) Central management over the web b) Classifies applications, users and devices c) Zero-touch, self-provisioning deployments d) Supports Zero-touch remote deployment e) Template based multi-network management f) Role based administration with change logging and alerts	
	10. **Network and Security** a) Auto Virtual Private Network (VPN) - self-configuring site-to-site b) Active Directory Integration c) Identity-based policies d) Client VPN (IPsec L2TP) e) Software Defined Wide Area Network (SD-WAN): Dual active VPN with policy based routing and dynamic path selection	
	11. **Traffic shaping and application management** a) Layer 7 application visibility and traffic shaping b) Application prioritization	
	12. **Advanced security services for two (2) years** a) Content filtering b) Intrusion Prevention System (IPS) c) Latest malware protection	
	13. **Remote Diagnostics** a) Live remote packet capture b) Real-time diagnostic and troubleshooting tools c) Aggregate event log with instant search d) Built-in feature	
	14. **Reporting and Monitoring** a) Throughput, connectivity monitoring and email alerts	

	b) VPN tunnel and latency monitoring c) Periodic emails with key utilization metrics d) Syslog integration	
	15. **Gartner certification for the leader and challenger quadrant or NSSLAB certified**	
	16. **Warranty**: three year Full lifetime hardware warranty, including renewals	
	17. **Documentation** The Contractor shall provide original User's Guide and Technical Manuals for each unit.	
IV.	**CONTRACTOR QUALIFICATION**	
	18. The Contractor shall have at least five (5) years of experience in supply, delivery, installation, testing and commissioning of network installations and cabling services including systems integration. The Contractor shall submit proof (as stated in its Articles of Incorporation) that the primary purpose of their enterprise is to provide the technical/Information and Communications Technology equipment and corresponding services.	
	19. The Contractor shall be a Certified Partner for the FIREWALL APPLIANCE / UNIFIED THREAT MANAGEMENT SYSTEM Brand	
	20. The Contractor shall submit the following certification issued by the manufacturer of the FIREWALL APPLIANCE / UNIFIED THREAT MANAGEMENT SYSTEM: a. endorsing the Contractor, to bid, sell, support & maintain the product being offered	
	b. that the Contractor provides after sales service and parts for all the required equipment, accessories and software included in this project in the next 5 years commencing from the date of contract. The certification shall include company names, addresses and contacts.	
	c. from its local office or through its regional hub that all equipment and software are brand new and up-to-date.	

	d. that the bidder is certified partner for five (5) years or more of the brand equipment.	
	21. The Contractor's Engineers shall have the following minimum qualifications for the installation of the FIREWALL APPLIANCE / UNIFIED THREAT MANAGEMENT SYSTEM: a) Cisco Certified Network Associate (CCNA) b) Cisco Certified Design Associate (CCDA) c) FIREWALL APPLIANCE/UNIFIED THREAT MANAGEMENT SYSTEM brand certified.	
	22. The Contractor's technical support personnel (at least 5 engineers) shall be certified by the FIREWALL APPLIANCE / UNIFIED THREAT MANAGEMENT SYSTEM manufacturer that they are qualified to support the FIREWALL APPLIANCE / UNIFIED THREAT MANAGEMENT SYSTEM.	
V.	**DELIVERY AND PAYMENT**	
	23. The Contractor shall deliver and implement the FIREWALL APPLIANCE / UNIFIED THREAT MANAGEMENT SYSTEM within sixty (60) calendar days upon receipt of Notice to Proceed (NTP).	
	24. Payments shall be made thirty (30) working days upon full implementation of the system and receipt of the invoice with complete requirements through List of Due and Demandable Accounts Payable (LDDAP). The list of documentary requirements needed for payment will be provided by the Office of Financial Management Services-Financial Resource Management Division (OFMS-FRMD) upon signing of the contract	
	25. All payments shall be inclusive of Value Added Tax (VAT) 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.

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