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 Enterprise Resource Planning System (ERPS) Endpoint Cybersecurity Solution
Reference No.	:	PB-GS-38-2018
ABC	:	PhP 10,000,000.00
Date	:	11 December 2018

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I. Technical Specifications (Section VII) – The Technical Specifications (Section VII) of the Bidding Documents is superseded by ANNEX A of this Supplemental/Bid Bulletin No. 1 after considering inputs from End-User, BAC Members and prospective bidders during the pre-bid conference on 10 December 2018.

The Bidding Documents is amended accordingly.

For the information and guidance of all concerned.

(Sgd.)
IMELDA M. PANOLONG
BAC Chairperson

ANNEX A
Technical Specifications
ENTERPRISE RESOURCE PLANNING SYSTEM (ERPS) ENDPOINT CYBERSECURITY SOLUTION

I.	**BACKGROUND** In line with the Department of Information and Communications Technology's (DICT) National Cybersecurity Plan 2022 (NCSP 2022) and its vision to achieve a "Trusted and Resilient Infostructure," the Department plans to enhance the security and resiliency of its Enterprise Resource Planning System (ERPS).	
II.	**OBJECTIVE** The Department intends to procure a one-year subscription for the following set of solutions: 1. Advanced Endpoint Protection 2. Web Application Firewall	
II.	**SCOPE OF WORK**	**Statement of Compliance**
1.	The Contractor shall supply, deliver, install and configure an **Advanced Endpoint Protection and Web Application Firewall** at DFA Main Building and DFA – ASEANA.	
2.	The **Advanced Endpoint Protection and Web Application Firewall** shall include licenses as follows: a) **Advanced Endpoint Protection** – 1500 Endpoints b) **Web Application Firewall**	
3.	The Contractor shall integrate the proposed Advanced Endpoint Protection to the connected threat defense of the Department.	
4.	The Contractor shall install and configure the Advanced Endpoint Protection license to 1500 endpoints.	
5.	The Contractor shall install and configure the Web Application Firewall to the ERPS' application servers network segment.	
6.	The Contractor shall provide free classroom training to ten (10) technical personnel of the OAMSS-ITCRD on installation, configuration, management and maintenance of the **Advanced Endpoint Protection and Web Application Firewall** after the installation of the Solutions.	
7.	The Contractor shall provide a user's guide and technical manual of the **Advanced Endpoint Protection and Web Application Firewall.**	

III.	**TECHNICAL SPECIFICATIONS**	
	A. Advanced Endpoint Protection	
	1. The Solution shall: a. provide an endpoint protection with the following features: anti-malware, endpoint application control, integrated data loss prevention, behavioral monitoring and vulnerability protection. b. protect endpoints from known and unknown malwares through advance detection techniques. c. provide protection to off-network endpoints through cloud intelligence. d. identify and block ransomware proactively based on its behavior. e. provide protection for browser-based attacks or exploits. f. provide a host-based firewall built in with the endpoint agent. g. provide a device control feature to limit access to external storage devices and resources. h. support web based management. i. provide virtual patching. j. provide endpoint application control. k. provide a single lightweight agent for the following modules: anti-malware, endpoint application control, integrated data loss prevention, behavioral monitoring and vulnerability protection. l. provide protection for unauthorized uninstallation and modification of agents.	
	2. Integration Requirements The Solution shall be able to: i. integrate with the Department's existing NGIPS, Deep Discovery Inspector and Server Security to establish a connected threat defense. ii. forward suspicious objects to Deep Discovery Inspector for validation and analysis. iii. receive updates from the connected threat defense.	
	B. Web Application Firewall	
	1. The Solution shall a. Protect the Department's ERPS web applications from attacks that target known and unknown exploits b. Protect applications from known vulnerabilities and from zero-day threats using multi-layered and correlated detection methods	

	c. Have four different deployment modes: Inline Transparent, True Transparent Proxy, Reverse Proxy and Non-Inline Sniffing d. Provide web user interface for management and reporting e. Support web services signatures, virtual patching and threat scoring and weighing f. Have layer 7 application DOS attack protection **g. Have 1.3 Gbps Throughput, Active- active, Active-Passive clustering, 6 (4 bypass), 4 SFP GE (non-bypass)** **h. Have 2 10G BASE-SR SFP+ Ports** i. Offer an Anti Virus (AV) solution without introducing additional software or hardware deployments and not through third party integration solution. j. Be detected by known search engines. k. Support built-in vulnerability scanner, third-party scanner integration and file upload scanning with AV and sandbox. l. Support Layer 7 server load balancing, HTTPS/SSL Offloading and HTTP compression m. Include appliance(s) or equipment, if necessary n. Have at least "recommended" rating from NSS Labs' latest report (2017) o. Have a rating of at least "challenger" on latest Gartner WAF report (2017) p. Have the latest ICSA Labs certification (2017)	

IV.	**CONTRACTOR'S QUALIFICATION**	
	1. The Contractor shall have at least two (2) Certified Security Engineers specific to the brand being offered. 2. The Contractor shall submit the following certifications issued by the manufacturer(s): a. Endorsing the Contractor, to bid, sell, support and maintain the product being offered; b. That all equipment are brand new and up to date. 3. The Contractor's technical engineers must be locally employed and shall submit the following proof of qualifications and employment: c. Certified True Copy of Company ID d. Certified True Copy of Certificate of Employment	

V.	**CONFIDENTIALITY CLAUSE**	
	The Contractor shall ensure that each of its personnel assigned to the Department shall execute and sign a Non-Disclosure Agreement which is to be submitted to the Department prior to the commencement of the Contract.	
VI.	**DELIVERY**	
	The contractor shall deliver, install and configure the **Advanced Endpoint Protection and Web Application Firewall** within forty-five (45) calendar days upon receipt of Notice to Proceed (NTP).	
VII.	**PAYMENT**	
	~~1. Payment shall be made upon complete delivery and installation of the **Advanced Endpoint Protection and Web Application Firewall.**~~ 1. The payment shall be made within thirty (30) working days **upon delivery and** full implementation of the system and receipt of the invoice with complete requirements through List of Due and Demandable Accounts Payable (LDDAP). 2. All payments shall be inclusive of all applicable taxes and other lawful charges.	

VIII.	**WARRANTY AND SUPPORT**	
	The Contractor shall provide: 1. A ~~one (1)~~ **two (2)** year warranty and support for all software, equipment and peripherals pertinent to the Solutions commencing on the complete installation of the **Advanced Endpoint Protection and Web Application Firewall;** 2. 24x7 technical support with four (4) hours response time and six (6) hours resolution time during the warranty period; 3. After sales services for a period of ~~one (1)~~ **two (2)** year commencing on the complete installation of **Advanced Endpoint Protection and Web Application Firewall;** 4. Quarterly Business Review (QBR) which shall include but not be limited to the submission of reports and analytics; and 5. A single point of contact for all technical inquiries/issues.	

Note:

Bidder must state compliance to each of the provisions in the Terms of Reference/Technical Specifications, as well as to the Schedule of 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 if 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 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 or 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 of 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]
[Position]
[Date]