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 Advance Cybersecurity (Secure Internet Gateway and Endpoint-Based Malware Protection)
Reference No.	:	PB-GS-05-2018
ABC	:	PhP 7,000,000.00
Date	:	12 March 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The Technical Specifications (Section VII) of the Bidding Documents is superseded by **ANNEX A** of this Supplemental/Bid Bulletin No. 2 after considering inputs from prospective bidders during the pre-bid conference on 09 March 2018.

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

ADVANCE CYBERSECURITY
(Secure Internet Gateway and Endpoint-Based Malware Protection)

I.	**OBJECTIVE** In line with 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 improve its mission-critical and non-critical infostructure security, in particular, cybersecurity. These initiatives will greatly enhance the security and resiliency of the Department's mission-critical and non-critical infostructure. The Department shall procure a nine-month subscription (01 April to 31 December 2018) for the following set of solutions for servers and endpoints: 1. Secure Internet Gateway (DNS Security) 2. Endpoint-Based Malware Protection	
II.	**SCOPE OF WORK**	**Statement of Compliance**
1.	The Contractor shall supply, deliver, install and configure a Secure Internet Gateway and an Endpoint-Based Malware Protection at DFA Head Office and Office of Consular Affairs.	
2.	The Contractor shall supply, install and configure all security appliances required for the implementation of the Secure Internet Gateway and the Endpoint-Based Malware Protection.	
3.	The Contractor shall ensure that Secure Internet Gateway and the Endpoint-Based Malware Protection Solutions are of similar brand.	
4.	The Secure Internet Gateway and Endpoint-Based Malware Protection shall include licenses as follows: a) Secure Internet Gateway – 1500 users b) Endpoint-based Malware Protection – 1500 Endpoints	
5.	The Contractor shall integrate the Secure Internet Gateway to the existing firewall of DFA Main Office and Office of Consular Affairs.	
6.	The Contractor shall provide free classroom training to ten (10) technical personnel of the DFA on installation, configuration, management and maintenance of the Secure Internet Gateway and Endpoint-Based Malware	

	Protection immediately after the installation of the Solutions.	
7.	The Contractor shall provide certification training for Certified Information Systems Security Professional (CISSP) for four (4) personnel of the Department at a CISSP-authorized training center.	
8.	The Contractor shall provide hard and soft copies of the user's guide and technical manual of the Secure Internet Gateway and Endpoint-Based Malware Protection.	
III.	**TECHNICAL SPECIFICATIONS**	
1.	**Secure Internet Gateway System Requirements**	
	1.1 Architectural Requirements The Solution shall: • be delivered and managed from cloud for scalability and flexibility; • be based on recursive DNS analysis; • enforce/apply threat intelligence at the DNS layer; • offer several deployment options: (e.g. internal virtual forwarder, pointing the forwarder of the existing authoritative DNS to the recursive service, or an endpoint agent); • provide a recursive DNS security service via a global data centre network; • ensure that the recursive DNS security is easily deployable and delivered directly from the vendor's global network; and • be available for wired and wireless network users.	
	1.2 Security Requirements The Solution shall: • provide protection from malware, especially from botnets, exploit kits, drive-by, phishing, newly seen domains, potentially harmful domains, DNS Tunnelling services; • provide predictive intelligence created via the DNS traffic analysis on a global scale, and via a network of distributed datacentres hosting the resolver; • send suspected malicious domains to a proxy service for further scanning; • allow the Department to create its own lists of blocked URLs; • enforce web filtering policies, based on categories; and	

	• allow, through its web filtering and security policies, the creation of global exceptions for several domains, via custom whitelists or blacklists.	

	1.3 Management Requirements
	The management interface shall:
	• be secure and web-based;
	• allow the creation of different user profiles with different levels of permission;
	• provide a graphical policy editor;
	• provide a dashboard that shows the following:
	  ○ global DNS activity on each configured site, identifying in real time the targeted attacks by comparing the local DNS traffic to a specific domain with the worldwide DNS traffic for the same domain,
	  ○ overview of all the traffic of the local organisation, with the ability to quickly pinpoint blocks related to security events and web filtering policy;
	• perform domain-based and lens-based reporting that allows to select a domain and show all its events over time, including the user identity;
	• generate reports based on web filtering or security categories being accessed which includes, but is not limited to, the following:
	  ○ Total requests;
	  ○ Activity volume;
	  ○ Top Domains;
	  ○ Top Categories;
	  ○ Top Identities;
	• export reports in csv format;
	• log all the activities made by administrators through an Admin Audit Log Report; and
	• provide 2-Factor Authentication mechanisms for the administrators.	

	1.4 Integration Requirements The solution shall: • extend the protection of the network through the installation of a lightweight roaming agent on Windows and OSX devices; • be deployable via Global Policy Object (GPO) through its roaming agent; and	

	• enforce security policies for malware hosted on both IP address and/or fully qualified domain name.	
	1.5 Resiliency and reliability requirements • The network used to deliver the DNS security service shall use Anycast and shall have an uptime of at least 99.9% over the last 10 years.	
2.	**Endpoint-based Malware Protection Requirements**	
	2.1 Architectural Requirements The Solution shall: • be delivered and managed from cloud for scalability and flexibility; • have a lightweight software footprint; and • co-exist with existing systems already deployed on the endpoints.	
	2.2 Security Requirements The Solution shall: • support both static and behavioural analysis of files; • perform root cause analysis with the following features: o sequential and chronological trace of events with details including host, username, IP, and client application; o details which files/processes/services are affected; • track malware movement and provide visualization at the network level (systems and users affected, patient zero, and method/point of entry); • continuously monitor and file retrospection to flag missed malware events without the need for rescan; • detect vulnerability of software installed in the endpoint machines; • support full file analysis in secure sandbox, with detailed report; • block dropper activity and contain the spread of malware; and • remediate endpoints which shall include, but not be limited to, the following features: o tracks and captures files; o blocks malicious files / processes / services; o submits suspected hash of malicious files for further analysis;	

	○ blocks malware based on custom black IP list; ○ blacklists/whitelists IPs and applications.	
	2.3 Integration Requirements The Solution shall extend protection to endpoints on the following platforms: a. Microsoft Windows 7 b. Microsoft Windows 8 and 8.1; c. Microsoft Windows 10; d. Microsoft Windows Server 2003; e. Microsoft Windows Server 2008; f. Microsoft Windows Server 2012; g. Mac OS X 10.7 and later versions; h. Linux Red Hat Enterprise 6.x and 7.x; i. Linux CentOS 6.x and 7.x; j. Android version 2.1 and later versions.	
IV.	**CONTRACTOR'S QUALIFICATION**	
	1. The Contractor shall have: a. at least ten (10) year experience in IT related business operations; b. **at least three (3) year experience in cybersecurity solutions**; c. at least three (3) year experience in supply, delivery, installation, testing and commissioning of security installation, including systems integration.	
	2. The Contractor shall submit the following certification/documentation issued by the manufacturer of the Solution to attest to the following: a. that the Contractor is a certified partner for at least three (3) years or more of the Solution; b. that the Contractor is authorized to bid, sell, support and provide maintenance for the Solution; and c. that the Contractor provides after sales service and parts for all the required equipment, accessories and software included in this project. The certification shall include company name, address and contacts.	

	3. The Contractor's engineers shall: a. **Have one each of the following qualifications** for the installation of the Secure Internet Gateway and Endpoint-Based Malware Protection: i. Cisco Certified Network Associate (CCNA - Security); ii. Cisco Certified Design Associate (CCDA); iii. Cisco Certified Network Professional (CCNP); and b. be locally employed and shall submit the following: i. Certified True Copy of Certificate of Employment; ii. Certified True Copy of Company ID.	
V.	**DELIVERY**	
	The Contractor shall deliver and implement the Secure Internet Gateway and Endpoint-Based Malware Protection within thirty (30) calendar days upon receipt of Notice to Proceed (NTP).	
VI	**CONFIDENTIALITY**	
	The Contractor shall ensure the confidentiality and integrity of the data and documents processed in the course of the implementation of the subscription.	
VII.	**PAYMENT**	
	1. The payment shall be made within thirty (30) working days upon full implementation of the system and issuance of licenses, 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.	
	2. All payments shall be inclusive of Value Added Tax (VAT) and other lawful charges.	
VIII.	**WARRANTY AND SUPPORT**	
	The Contractor shall provide: • **Twelve (12) months** ~~Nine (9) months~~ warranty support and services; • 24/7 technical/customer support, four (4) hours response and six (6) hours resolution time during the warranty period;	

	• a single point of contact assigned to the DFA for all technical inquiries/issues; • Quarterly Business Review (QBR) which shall include, but not be limited to, submission of reports and analytics; and • After sales support in the next 5 years commencing from the date of contract.	

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 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 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 or supplier liable for prosecution subject to the provisions of **ITB** Clause **Error! Reference source not found.** and/or **GCC** Clause **Error! Reference source not found.**.

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