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 Cybersecurity Management System for the Enterprise Resource Planning System (ERPS) Endpoint
Reference	:	PB-GS-10-2019
ABC	:	PhP 7,300,000.00
Date	:	17 September 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I. **Technical Specifications (Section VII)** – The Technical Specifications (Section VII) of the Bidding Documents is superseded by ANNEX A of this Supplemental/Bid Bulletin No. 1 after considering correction of typographical error.

The Bidding Documents is amended accordingly.

For the information and guidance of all concerned.

(sgd.)
IMELDA M. PANOLONG
BAC Chairperson

ANNEX A
Technical Specifications

Procurement of Cybersecurity Management System for the Enterprise Resource Planning System (ERPS) Endpoints

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 enhance the security and resiliency of its Enterprise Resource Planning Solution (ERPS) and all endpoints using the ERPS. In this regard, the Department shall procure a one-year subscription of **Cybersecurity Management System** for the endpoints using the ERPS with the following components: 1. **Security Information and Event Management (SIEM)**; and **2. Vulnerability Management (VM)**	
II.	**SCOPE OF WORK**	**Statement of Compliance**
1.	The Contractor shall supply, deliver, install and configure a **Cybersecurity Management System (CMS)** for all endpoints using the ERPS at the DFA Head Office and Office of Consular Affairs, with the following components: 1. **Security Information and Event Management (SIEM);** and 2. **Vulnerability Management (VM)**	
2.	The Contractor shall supply, install and configure all the security appliances required for the implementation of the **SIEM and VM** at no additional cost to the End-User.	
3.	The **SIEM and VM** shall include the following licenses: a) SIEM Collector appliance; b) SIEM license for 800 ICT assets; and c) Vulnerability Management.	
4.	The Contractor shall integrate the **SIEM and VM** to all ERPS enpoints and existing cybersecurity tools.	
5.	The Contractor shall provide certification training to five (5) OAMSS-ICTD personnel on the **SIEM and VM**.	
6.	The Contractor shall provide as-built documentation of the **SIEM and VM.**	
III.	**TECHNICAL SPECIFICATIONS**	
1.	**Security Information and Event Management**	
	The Solution shall provide: a) twelve (12) million security events per day to be processed and analyzed; b) license and capacity for growth of security events until Day 0+12 months; c) license for 800 honey credentials deception technology; d) license for 800 file deception technology e) license for 800 honey server deception technology; and	

	f) license for 800 honey user deception technology.	
	1.2 Inventory and Control of Hardware Assets The solution shall have: • visibility to all active endpoints in the infrustracture via Agentless Scan or Agent installation; and • a central console for configuration of automated or manual remediation which shall include process termination and/or quarantine asset. **1.3 Inventory and Control of Software Assets** The solution shall display endpoint information such as Operating System, Running processes, Authentications and Account information. **1.4 Continuous Vulnerability Management** The solution shall: • continuously monitor the following: - Malware Application process based on multiple reputable databases - Attacker **Behavior** in the whole infrastructure • detect leaked credentials; • detect password guessing attempts; • detect switching of identities; • detect unusual authentications beyond baseline; • identify privilege escalation; • detect powershell executions; • detect multiple country authentications; • automatically baseline behavior of users; • provide an automated alert correlation with data from the following but not limited to: - CERT feed - FBI feed - Phishing IOC feed - TOR exist node feed - Abuse .ch feed - Crytocurrency miner feedlist - Cryptolocker feedlist • manually add localized based feeds to match and correlate with for alerts. **1.5 Controlled Use of Administration Privileges** The solution shall: • list all administrative accounts, including domain and local accounts; • log and alert on changes to Admin group membership; • log and alert when an account is added to any group assigned administrative privileges; • log and alert unsuccessful administrative account login; and	

	• support multi-factor out-of-band authentication such as SMS Authentication and Google authenticator. **1.6 Maintenance, Monitoring and Analysis of Audit Logs** The solution shall: • ingest, analyze and correlate audit logs from all systems and networking devices such as Active Directory, LDAP, Windows, MAC and Proxy Server; • keep detailed log information such as event source, date, username, timestamp, source address, and other useful elements; • hunt for anomalies or abnormal events; and • provide built-in incident and response tracking system wherein the SOC head can assign incident to designated analysts for resolution. **1.7 Email and Web Browser Protectors** The solution shall: • store outbound URL request and detect access to malicious domains; • obtain intelligent threat feeds from multiple reliable sources on the internet; • create their own threat feed to detect attacker activity; and • define owned domains to detect spear phishing. **1.8 Malware Defenses** The solution shall: • ingest DNS query logs and detect hostname lookups for known malicious domains; • ingest command-line audit logs from command shells; • ingest and generate alerts for malware detection based on anti-malware system such as Trend Micro Office scan and Trend Micro Control Manager; and • detect malware/ malicious hash on process or code behavior executing in every users' system. **1.9 Limitations and Control of Network Ports, Protocols and Services** The solution shall: • detect services running on their endpoint; • ingest firewall logs and generate alerts to the Department's existing firewall; and • backup the log data either on cloud or on premise. **1.10 Boundary Defense** The solution shall: • define network zones and policies to monitor employee access to restricted zones or disorder intruder attempts via accounts;	

	• detect communications with known malicious or unused internet IP addresses and limit access only to trusted IP range at each of the organization's network boundaries; • detect unauthorized application traffic; • ingest logs from the Department's existing Intrusion Prevention System (IPS); • detect enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices; and, • monitor access to authorized cloud applications/ storage and detect users accessing non-authorized usage. **1.11 Controlled Access Based on the Need to know** The solution shall: • detect lateral movement and remediate when necessary by disabling user or putting asset in quarantine; • track file event logs, such as when a file is edited, moved, or deleted and attribute this file modification activity to user files such as .bat, .exe, .conf, .dll, .sys and others; and • perform log collection for flat file logs. **1.12 Account Monitoring and Control** The solution shall: • monitor and check that all accounts have an expiration date; • detect lateral movement and remediate when necessary by disabling user or putting asset in quarantine; • monitor attempts to access deactivated accounts; • log and alert on unsuccessful administrative account login; and • alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration. **1.13 Incident Response and Management** The solution shall: • generate alerts at different levels of granularities based on a variety of parameters; and • assign job titles and duties for handling computer and network incidents to specific individuals and ensure tracking and documentation throughout the duration of the incident until its resolution.	
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; and 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: a. Certified True Copy of Company ID b. Certified True Copy of Certificate of Employment 4. Supporting Certifications shall be included as part of the Contractor's bid.	
V.	**DELIVERY**	
	The Contractor shall deliver, install and configure the **Cybersecurity Management System for ERPS Endpoints** within forty-five (45) calendar days upon receipt of Notice to Proceed (NTP).	
VI.	**PAYMENT**	
	1. The payment shall be made within 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). 2. All payments shall be inclusive of all applicable taxes and other lawful charges.	
VII.	**WARRANTY AND SUPPORT**	
	The Contractor shall provide: 1. Warranty and support for all software, equipment and peripherals pertinent to the Solutions for a period of one (1) year commencing on the implementation date of the **Cybersecurity Management System for ERPS Endpoints.** 2. 24x7 technical support with four (4)-hour response time and six (6)-hour resolution time during the warranty period; 3. After sales services for a period of one (1) year commencing on the delivery date of **Cybersecurity Management System;** 4. Quarterly Business Review (QBR) including, but not limited to, submission of reports and analytics; 5. A single point of contact for all technical inquiries/issues; and	

	6. An original User's Guide and Technical Manual for the **Cybersecurity Management System.**	

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]