REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF BUDGET AND MANAGEMENT
GENERAL SOLANO STREET, SAN MIGUEL, MANILA

SUPPLEMENTAL/BID BULLETIN (SBB) NO. 1

This SBB No. 1 dated March 10, 2020 for the Project, "Subscription of Advanced Endpoint Security Solution," is issued to clarify, modify or amend items in the Bidding Documents. Accordingly, this shall form an integral part of said Documents.

PARTICULARS		**CLARIFICATION/AMENDMENTS**	
Section VII. Technical Specification xxxx		**Section VII. Technical Specification** xxxx	
Specifications	**Bidder's Statement of Compliance**	**Specifications**	**Bidder's Statement of Compliance**
I. Objective *(see attached Annex A, item II)*		I. Objective *(see attached **Revised** Annex A, item II)*	
II. Delivery Period *(see attached Annex A, item III)*		II. Delivery Period *(see attached **Revised** Annex A, item III)*	
III. Specifications *(see attached Annex A, item IV)*		III. Specifications *(see attached **Revised** Annex A, item IV)*	
IV. Scope of Work *(see attached Annex A, item V)*		IV. Scope of Work *(see attached **Revised** Annex A, item V)*	
V. Service Level Agreement *(see attached Annex A, item VI)*		V. Service Level Agreement *(see attached **Revised** Annex A, item VI)*	
VI. Warranties of the Contractor *(see attached Annex A, item VII)*		VI. Warranties of the Contractor *(see attached **Revised** Annex A, item VII)*	
VII. Confidentiality of Data *(see attached Annex A, item VIII)*		VII. Confidentiality of Data *(see attached **Revised** Annex A, item VIII)*	
VIII. Terms of Payment *(see attached Annex A, item IX)*		VIII. Terms of Payment *(see attached **Revised** Annex A, item IX)*	
IX. Pre-Termination of Contract *(see attached Annex A, item X)*		IX. Pre-Termination of Contract *(see attached **Revised** Annex A, item X)*	

	Attached are the Revised Section VII. Technical Specifications and the Revised Annex "A"

Other matters:

- The "No Contact Rule" shall be strictly observed. Bidders are not allowed to call or talk to any member of the Bids and Awards Committee, Technical Working Group or, Secretariat effective March 17, 2020 right after the opening of bids.

- For guidance and information of all concerned.

ACHILLES GERARD C. BRAVO
Assistant Secretary
Chairperson, DBM-BAC

Section VII. Technical Specifications

(Revised)

Bidders must state here either "Comply" or any equivalent term in the column "Bidder's Statement of Compliance" against each of the individual parameters of each "Specification."

Specifications	Bidder's Statement of Compliance
I. Objective *(see attached Revised Annex A, item II)*	
II. Delivery Period *(see attached Revised Annex A, item III)*	
III. Specifications *(see attached Revised Annex A, item IV)*	
IV. Scope of Work (*see attached Revised Annex A, item V)*	
V. Service Level Agreement (*see attached Revised Annex A, item VI)*	
VI. Warranties of the Contractor (*see attached Revised Annex A, item VII)*	
VII. Confidentiality of Data (*see attached Revised Annex A, item VIII)*	
VIII. Terms of Payment *(see attached Revised Annex A, item IX)*	
IX. Pre-Termination of Contract (*see attached Revised Annex A, item X)*	

I hereby certify to comply with all the above Technical Specifications.

Name of Company/Bidder **Signature Over Printed Name of Representative** **Date**

Annex "A"

TECHNICAL SPECIFICATION
(Revised)

I. PROJECT TITLE

Subscription of Advanced Endpoint Security Solution

II. OBJECTIVE

To implement a comprehensive and advanced endpoint security platform based on next generation cybersecurity technologies, endpoint detection and response, unknown malware analysis and managed protection for the DBM users' end devices and application servers.

III. DURATION OF THE CONTRACT

The contract duration for the subscription shall be twelve (12) months from the issuance of Certificate of Acceptance.

IV. SPECIFICATIONS

4.1 Endpoint

4.1.1 The proposed solution must be able to support a wide range of Windows operating systems including Windows Servers 2016.

4.1.2 The proposed solution must be able to support MacOS and Linux including Linux Containers.

4.1.3 The proposed solution must be able to support both Workstations, Servers and Android with single license.

4.1.4 The proposed solution must be a signature-less solution.

4.1.5 The proposed solution must be Microsoft Windows Security Center Certified or recognized.

4.1.6 The proposed solution must able to protect proprietary applications such as in-house applications.

4.2 Management

4.2.1 The proposed solution must be cloud based management

4.2.2 The proposed solution shall have the capability to report all security incidents back to management immediately as long as the endpoint is connected to the management.

4.2.3 The proposed solution shall provide Web-based Graphical User Interface (GUI).

4.2.4 The proposed solution management shall also able to manage policy for mobile (e.g. Android) in one single console.

4.2.5 The proposed solution management shall allow user to upgrade endpoint without third party software or tool.

4.2.6 The proposed solution management shall provide malware file report view online or download as pdf.

4.2.7 The proposed solution management shall provide capability for administrator to create exception directly from security event.

4.2.8 The proposed solution management shall provide 2FA capability without need of customer integration.

4.2.9 The proposed solution shall provide grouping capability as following but not limited to:

- Static – select from existing connected endpoints
- Dynamic – by define condition based on Endpoint name, Domain, IP Addresses, VDI, agent version, and the Operating System on Endpoints.

4.3 Integration

4.3.1 The proposed solution shall provide the capability to get intelligence feed from the existing Palo Alto Networks firewall without any additional custom integration or configuration.

4.3.2 The proposed solution shall provide capability to integrate with on-premises Active Directory.

4.3.3 The proposed solution shall provide capability to forward logs to SIEM or Syslog server.

4.3.4 The proposed solution must have sandbox capability.

4.3.5 The proposed solution must be compatible with the existing Palo Alto Network Security Solution in order to provide full visibility in all network traffic (inbound and outbound).

4.4 Exploit Prevention

4.4.1 The proposed solution shall provide the prevention against exploit kit that do fingerprinting through browser (e.g. Internet Explorer and Edge)

4.4.2 The proposed solution shall provide prevention against exploit that attack the operating system kernel through kernel privilege escalation.

4.4.3 The proposed solution shall prevent attacks which change the execution order of a process by redirecting an asynchronous procedure call (APC) to point to the attacker's malicious shellcode

4.4.4 The proposed solution shall be able to provide real-time prevention against exploits of application vulnerabilities by blocking through core exploit techniques not limited to Software Logic Flaws, Memory Corruptions, code execution, DLL Hijacking, etc.

4.4.5 The proposed solution must be able to protect the systems without knowing the CVE numbers

4.4.6 The proposed solution shall prevent zero-day or undiscovered exploits of any application vulnerabilities by blocking through core exploits techniques.

4.4.7 The proposed solution should provide the capability to perform exploit monitoring and prevention based on core exploit techniques without connection to the Management Server and/or Cloud Service or without relying on signatures.

4.4.8 The proposed solution shall collect forensic data like process name, file source and path, time stamp, memory dump, operating system version, user ID, vulnerable application version while terminate the particular process that under attack.

4.4.9 The proposed solution shall utilize core exploit technique to prevent or block. It shall not be based on signatures or reputation of the file.

4.4.10 The exploit technique modules shall be able to apply to known and popular applications as well as authorized unknown or in-house developed applications.

4.4.11 The proposed solution shall provide protection against exploit including MacOS, Windows, Linux and processes running in Linux Containers.

4.4.12 The proposed solution shall provide automated forensic memory dump analysis to allow administrators to quickly understand exploit events.

4.4.13 The proposed solution shall also provide Behavior Analytics capability to prevent or block suspicious activities which may or may not related to exploit.

4.5 Malware Prevention

4.5.1 The proposed solution shall provide protection against malicious DLL files

4.5.2 The proposed solution shall provide anti-ransomware capability through creation of decoy file and not using customer live file.

4.5.3 The proposed solution shall support protection against the execution of malicious executables.

4.5.4 The proposed solution shall have the capability to restrict files and applications execution on or from local folder, network folder, external media (e.g. USB Drive and Optical Media).

4.5.5 The proposed solution shall have the capability to restrict files and applications from loading another process that is unknown or in the background (a.k.a child processes)

4.5.6 The proposed solution shall use signature-less type of technology to prevent malware.

4.5.7 The proposed solution shall use dynamic analysis technology (e.g. Sandbox) to identify unknown malicious executables including DLL.

4.5.8 The proposed solution shall use Machine Learning technology to prevent malware on Windows, Mac OS, Linux, Linux Containerized processes, and Android.

4.5.9 The proposed solution shall have multi-layer prevention technology that includes but not limited to sandbox, machine learning and restriction.

4.6 Unknown Malware Analysis

4.6.1 The proposed solution shall include cloud sandbox with NO additional cost.

4.6.2 The proposed solution shall have capability to prevent unknown or zero-day malware when the endpoint is in offline stage (no internet or management connection).

4.6.3 The proposed solution shall have the capability to prevent unknown file or application through restriction policy.

4.6.4 The proposed solution shall have the capability to prevent unknown file from executing until the file is been verify.

4.6.5 The proposed solution shall have the capability to prevent executables file by customer provided hashes.

4.6.6 The proposed solution shall have the capability to identify and prevent greyware

4.6.7 The proposed solution shall automatically submit unknown file to sandbox without the need of administrator intervention.

4.6.8 The proposed solution shall have the capability to quarantine unknown and zero malware.

4.6.9 The proposed solution shall be able to identify and prevent sophisticated attacks that utilize legitimate processes and actions for malicious activity based on run-time behavior.

4.7 Detection and Response

4.7.1 The proposed solution shall allow security administrator to hunt using Indicator of Compromise or Combine of multiple behavior of the Indicator.

4.7.2 The proposed solution shall has capability to display the attack timeline.

4.7.3 The proposed solution shall has the capability to show the suspicious file was loaded or launch by which parent processes.

4.7.4 The proposed solution shall not limit to only endpoint but also able to show and correlate network data from firewall.

4.7.5 The proposed solution shall provide the behavior recording capability like network and user behavior analysis through solution provided sensors and not through Netflow data.

4.7.6 EDR, network user behavior analysis and Prevention should be single endpoint agent.

4.7.7 The proposed solution shall has the capability to isolate the endpoint.

4.7.8 The proposed solution shall has capability to blacklist suspicious file from the investigation console.

4.7.9 The proposed solution shall able to profile the environment for behavior detection base on but not limited to peer, time and entity.

4.7.10 The proposed solution shall be able to detect behavior as following but not limit to:

- Command and Control
- Reconnaissance
- Lateral Movement
- Data Exfiltration

4.7.11 The proposed solution Network and User behavior analysis shall not be based on Net Flow. It shall base on AI or Machine Learning technology with combine of Endpoint, Logs and Networks.

4.7.12 The proposed solution shall be able to detect file-less attack and script base attack.

4.7.13 The proposed solution shall provide query builder for threats hunting base on the following but not limited to:

- Process
- File
- Hash (MD5 and SHA256)
- Network (IP addresses, port, protocol, country)
- Registry
- Signer

4.7.14 The proposed solution shall be able to provide the visualization flow of the chain of events. It must include processes in the chain that happen before the malicious process.

4.7.15 The proposed solution shall be able to create behavior indicators to identify malicious intent

4.7.16 The proposed solution shall be able to detect threats on unmanaged device or network anomalies based on peer behavior.

4.7.17 The proposed solution must have the capability to chain detection from network, endpoint and cloud.

4.7.18 The proposed solution shall allow administrator to create custom detection rules to adapt based on environment.

4.7.19 The proposed solution shall have live remote and remote isolation as response.

4.7.20 The proposed solution shall have process termination capability.

4.7.21 The proposed solution shall have the capability to assign and mark the stage of investigation of specific incident.

4.8 Reporting

4.8.1 The proposed solution shall have a natively built-in dashboard to monitor the following:

- Unresolved Security Events in the defined timeframe with different severities.
- The OS platform and the number of managed agents.
- The endpoint license consumption status and its expiry date.

4.8.2 The proposed solution shall be able to monitor the health of the individual endpoints including but not limited to:

- Endpoint Hostname
- User
- Status
- Underlying OS
- Agent Version
- Last Seen Time

4.8.3 The proposed solution shall provide a high-level summary of the security and deployment status of endpoints. The report can be scheduled to run on a recurring basis and on-demand. The report shall be able to optionally send to one or more e-mail addresses.

4.9 Forensics

4.9.1 The proposed solution shall support the collection of forensic data captured by the advanced endpoint solution to a centralized location.

4.9.2 The proposed solution shall support automatic collection of the following forensic information for further investigation purposes:

- Memory Dump
- Accessed Files
- Loaded Modules
- Accessed URI
- Ancestor Processes

4.9.3 The proposed solution shall have the capability to view high level system information about the endpoint after the threat has been detected and also provide the capability to retrieve the prevention data for further analysis and investigation.

V. SCOPE OF WORK AND SERVICES

5.1 The CONTRACTOR shall conduct pre-implementation meeting with DBM representatives and current Facility Management Service provider so that all the necessary preparations, ideal set-up, contractor's familiarization of the computing environment, and other implementation matters are clearly discussed and finalized.

5.2 The CONTRACTOR shall deliver, install, configure and make operational the Advanced Endpoint Security Solution and its components for 1,500 devices (servers, workstations and mobile devices) within sixty (60) calendar days from receipt of Notice to Proceed (NTP).

The CONTRACTOR must have the following Certified Professionals for the Advanced Endpoint Security Solution installation, configuration, testing, commissioning and integration with Network

Access Control (NAC) and alignment to the DBM enterprise network (certificates must be submitted in the submission of bid documents and subject for post qualification):

- Manufacturer-Certified Advanced Endpoint Security Professional or its equivalent
- CISCO Certified Network Professional

5.3 Technical Support

5.3.1 The CONTRACTOR must be able to provide a 3-tier support:

- Local reseller as the first-level of support
- Distributor as the second-level of support
- Principal as the third-level of support

5.3.2 The CONTRACTOR shall provide/render twenty-four hours a day, seven days a week (24x7) technical support service that can be delivered in a form of telephone call, electronic mail, and/or on-site support.

The CONTRACTOR shall resolve every problem within six (6) hours after it was reported by DBM. It shall refer to a condition wherein the reported problem is resolved by the CONTRACTOR to the satisfaction of the DBM. Problem and resolution shall be logged in the DBM Help Desk Facility.

5.4 The CONTRACTOR shall provide Technology Transfer based on the following schedule:

Training	Schedule	No. of Participants	Duration
Advanced Endpoint Security Solution installation, configuration and administration	To be scheduled by the DBM-ICTSS prior to the engagement of the contract.	At least five (5) ICTSS personnel.	One (1) day
	To be scheduled by the DBM-ICTSS prior to the engagement of the contract.	At least five (5) ICTSS personnel.	One (1) day
	To be scheduled by the DBM-ICTSS prior to the engagement of the contract.	At least five (5) ICTSS personnel.	One (1) day

The CONTRACTOR shall issue individual training certificates and training materials for each of the participants.

5.5 The CONTRACTOR shall provide as-built documentation of the Advanced Endpoint Security Solution set-up/ diagram in both hard and soft copies including information in the deployment, system resource/overhead requirements of the software/IT equipment employed in the project as well as procedures for installation, configuration, integration, usage and backup within sixty (60) calendar days from the receipt of NTP.

5.6 A Certificate of Acceptance shall be issued by the Director of Information and Communication Technology Systems Service (ICTSS).

VI. SERVICE LEVEL AGREEMENT

6.1 DBM shall maintain a Service Level Agreement (SLA) with the CONTRACTOR, with provisions for liquidated damages for their non-compliance.

Component	Description	Liquidated Damages
6.1.1 Delivery, Installation, Configuration and Operationability	The CONTRACTOR shall deliver, install, configure and make operational the Advanced Endpoint Security Solution and its components for 1,500 devices (servers, workstations and mobile devices) within sixty (60) calendar days from receipt of Notice to Proceed (NTP).	One (1) % of the total contract price shall be imposed for everyday of delay.
6.1.2 Technical Support	The CONTRACTOR shall provide/render twenty-four hours a day, seven days a week (24x7) technical support service that can be delivered in a form of telephone call, electronic mail, and/or on-site support. The CONTRACTOR shall resolve every problem within six (6) hours after it was reported by DBM. It shall refer to a condition wherein the reported problem is resolved by the CONTRACTOR to the satisfaction of the DBM. Problem and resolution shall be logged in the DBM Help Desk Facility.	1/10th of 1% of the total contract price shall be imposed for every hour of delay. Said penalty shall be deducted from the special bank guarantee.
6.1.3 Technical Training	The CONTRACTOR shall provide Technology Transfer based on the schedule that will be provided by DBM-ICTSS prior to the engagement of the contract.	1/10th of 1% of the total contract price shall be imposed for every day of delay. Said penalty shall be deducted from the special bank guarantee.
6.1.3 Documentation	The CONTRACTOR shall provide as-built documentation of the Advanced Endpoint Security Solution set-up/ diagram in both hard and soft copies including information in the deployment, system resource/overhead requirements of the software/IT equipment employed in the project as well as procedures for installation, configuration, integration, usage and backup within sixty (60) calendar days from the receipt of NTP.	1/10th of 1% of the total contract price shall be imposed for every day of delay. Said penalty shall be deducted from the special bank guarantee.

VII. WARRANTIES OF THE CONTRACTOR

7.1 The CONTRACTOR warrants that it shall conform strictly to the terms and conditions of this TOR.

7.2 The CONTRACTOR warrants, represents and undertakes reliability of the services and that their manpower complements are hardworking, qualified/reliable and dedicated to do the service required to the satisfaction of the DBM. It shall employ well-behaved and honest employees with ID displayed conspicuously while working within the compound. It shall not employ DBM employees to work in any category whatsoever.

7.3 The CONTRACTOR in the performance of its services shall secure, maintain at its own expense all registration, licenses or permits required by National or Local Laws and shall comply with the rules, regulations and directives of Regulatory Authorities and Commissions.

7.4 The CONTRACTOR's personnel shall take all necessary precautions for the safety of all persons and properties at or near their area of work and shall comply with all the standard and established safety regulations, rules and practices.

7.5 The CONTRACTOR shall coordinate with the authorized and/or designated DBM personnel in the performance of their jobs.

7.6 The CONTRACTOR shall be liable for loss, damage or injury due directly or indirectly through the fault or negligence of its personnel. It shall assume full responsibility thereof and the DBM shall be specifically released from any and all liabilities arising therefrom.

7.7 The CONTRACTOR shall neither assign, transfer, pledge, nor sub-contract any part or interest therein.

7.8 The CONTRACTOR shall identify the certified technical support personnel that will be given authority to access and operate the specified equipment. DBM shall be informed thru a formal notice on the change or replacement of technical personnel five (5) days prior the actual rendering of technical support services.

7.9 The CONTRACTOR shall provide a services which shall include technical support and technology transfer which shall be covered by special bank guarantee equivalent to 10% of the total contract price. The said amount shall be released after the lapse of the subscription period. Provided that all conditions imposed under the contract have been fully met.

The subscription period shall commence on the day the DBM issues the Certificate of Acceptance.

VIII. CONFIDENTIALITY OF DATA

8.1 All project personnel of CONTRACTOR shall be required to sign a Non-Disclosure Agreement (NDA).

8.2 The CONTRACTOR agrees to hold the Proprietary Information in strict confidence. The CONTRACTOR furthermore agrees not to reproduce, translate or disclose the Proprietary Information to 3rd parties without prior written approval of the DBM.

IX. TERMS OF PAYMENT

9.1 The CONTRACTOR shall be paid upon provision of licenses and support services of this Project subject to the required Final Withholding VAT (Services) of five percent (5%) and Expanded Withholding Tax of two percent (2%).

9.2 Payment shall be made within a reasonable time from the submission of the documentary requirements such as, but not limited to the following, based on existing accounting and auditing laws, rules and regulations:

9.2.1 Sales Invoice/Billings
9.2.2 Training Certificate and Manual
9.2.3 Documentation
9.2.4 Certificate of Acceptance issued by ICTSS Director
9.2.5 Non-Disclosure Agreement

9.3 No advance payment shall be made as provided for in Section 88 of PD 1445.

X. *PRE-TERMINATION OF CONTRACT*

10.1 The contract for the Renewal of Licenses for the Subscription of Advanced Endpoint Security Solution may be pre-terminated by the DBM for any violation of the terms of the contract. In case of pre-termination, the CONTRACTOR shall be informed by the DBM thirty (30) days prior to such pre-termination.

10.2 In case of pre-termination, the CONTRACTOR shall be liable to an additional liquidated damages equivalent to one percent (1%) of the contract price as provided by the Government Accounting Manual (GAM) and forfeiture of the Performance Security.

10.3 The DBM shall have the right to blacklist the CONTRACTOR in case of pre-termination.