Republic of the Philippines
Office of the President

PHILIPPINE SPORTS COMMISSION

BAGONG PILIPINAS

REQUEST FOR QUOTATION

Date: June 30, 2025
P.R. No. ADMIN 2025-06-16-001

Name of Company:_____

Address:_____

Name of Store/ Shop:_____

Address: _____

TIN: _____

PhilGEPS Registration Number:_____

The **Philippine Sports Commission**, through its Bids and Awards Committee, intends to procure the **"Subscription of Advance Endpoint Security Solution for the Philippine Sports Commission"** accordance with ***Section 53.9 Small Value Procurement*** of the 2016 Revised Implementing Rules and Regulations of Republic Act No. 9184.

Please quote your best offer for the item described herein, subject to the Terms and Conditions provided at the last page of this RFQ. Submit your quotation duly signed by you or your duly authorized representative **not later than July 3, 2025 at 05:00 PM.** A copy of the following documents is required to be submitted, directly to the Bids and Awards Committee Office located at Room 207, Administration Building, RMSC, P. Ocampo Sr. St., Malate Manila:

A. PHILGEPS Registration or PHILGEPS Certificate
B. Omnibus Sworn Statement (notarized)
C. 2025 Mayor's/Business Permit
D. Income Tax Return (ITR) For 2024

Quotations must be properly labeled with reference number on the project offered. In case the deadline falls on a non-working day, legal holiday, or special non-working holiday the deadline shall be on the next working day.

For any clarification, you may contact us at Telephone No. 8 523-9831 loc.143 or email address pscprocurement@yahoo.com, procurement@psc.gov.ph and copy bac@psc.gov.ph

DR. CHRISTOPHER B. GACUTAN
BAC Vice Chairperson
Bids and Awards Committee

INSTRUCTIONS:

(1) Accomplish this RFQ correctly and accurately
(2) Do not alter the contents of this form in any way.
(3) All Technical Specifications are mandatory. Failure to comply with any of the mandatory requirements will disqualify your quotation.
(4) Failure to follow these instructions will disqualify your entire quotation.

After having carefully read and accepted the Terms and Conditions, I/We submit our quotation/s for the item/s as follows:

	Statement of Compliance		
TECHNICAL SPECIFICATIONS:	YES	NO	REMARKS
PROJECT NAME: **Subscription of Advance Endpoint Security Solution for the Philippine Sports Commission**			
Item 1			
Subscription of Advanced Endpoint Security			
Solution (12 Months Subscription) –			
421 LICENSES			
>Business Security Enterprise			
>Ransomware Mitigation			
>Management Console Cloud			
>Endpoint Security for Physical and Virtual workstations and Servers			
>Local and Cloud Machine Learning			
>Device Control			
>Application Blacklisting			
>Web Threat Protection			
>Automatic Disinfection and Removal			
>Endpoint Risk Analytics (ERA) (Cloud)			
>Advance Anti-Exploit			
>Network Attack Defense			
>Process Inspector			
>Endpoint Firewall with IDS			
>Fileless Attack Defense			
>Smart Centralized Scanning			
>Hyper Detect (Tunable Machine Learning)			
>Sandbox Analyzer			
>Incident Visualization			
>Root Cause Analysis			
>Anomaly Defense			
>MITRE Event Tagging			
>Endpoint Detection and Response (EDR)			
Supported Operating System			
>Windows Server 2022 Core			
>Windows Server 2022			
>Windows Server 2019 Core			
>Windows Server 2019			
>Windows Server 2016 Core			
>Windows Server 2016			
>Windows 11 Update (23h2) and earlier			
>Windows 10 Update (22h2) and earlier			
>Windows 10 IoT Enterprise			
>Microsoft Exchange Server 2019/2016/2013			

>macOS Sonoma (14.x)			
>macOS Ventura (13.x)			
>macOS Monterey (12.x)			
>macOS Big Sur (11.x)			
>Red Hat Ent. 7.0 and above			
>CentOS 7.0 or higher			
>Ubuntu 16.04 or higher			
>SUSE Ent. Server 11 SP4 or higher			
>OpenSUSE Leap 15.4-15.5			
>Fedora 37 or higher			
Endpoint Protection			
>The solution must have a local and cloud machine learning that provides predictive detection of unknown malware, dynamic file analysis trained on billions of samples, local machine learning trained on 80,000 malware features, and threat intelligence from over 500million endpoints globally.			
>Shall provide advanced anti-exploit that focuses on attack tools and techniques to detect both known and zero-day exploits that target browsers and popular software applications.			
>Shall provide fileless attack protection to detect and block fileless malware at pre-execution, including terminating PowerShell running malicious command line, blocking malicious traffic , analyzing memory buffer prior to code injection, and blocking the code injection process.			
>Shall provide network attack defense that focuses on detecting network attacks designed to gain access on endpoints through specific techniques such as brute-force attacks, network exploits, password stealers, drive-by-download infection vectors, bots, and trojans.			
>Shall provide ransomware vaccine that immunizes machines against known ransomware blocking the encryption process even if the computer is infected.			
>Shall provide ransomware mitigation that uses detection and remediation technologies to keep files from ransomware attack.			
>Shall provide the capability to automatically create backup copies of the files up to 15 MB in size, or smaller and restore them to their original location in case of ramsomware infections			
>The proposed solution must have a dedicated virtual machine that deduplicates and centralizes most of the antimalware functionality of antimalware agents, acting as a scan server.			
>Shall provide a next-gen tunable machine learning technology designed specifically to detect advanced attacks and suspicious activities in the pre-execution phase.			
>Shall provide web threat protection that scans incoming web traffic, including SSL, HTTP and HTTPSs traffic, to prevent the download of malware to the endpoint. Automatically blocks phishing and fraudulent web pages. Displays search ratings signaling trusted and untrusted pages.			
>The solution shall prevent sensitive data leakage and malware infection on attached devices by applying rules and exclusions via policy such as block, allow, and via custom rules.			
>The solution should provide full visibility and control of running applications by blacklisting unwanted software. Helps limit the risk of malicious code running undetected.			
>The solution shall provide fully featured two-way firewall that controls applications access to the network and to the internet. Furthermore, the firewall can protect the system against port scans, restrict ICS and warn when new nodes join a Wi-Fi connection.			
>The solution should provide data protection that allows blocking of confidential data (pin card, bank account, etc.) for both HTTP and SMTP, by creating specific rules.			
>Shall provide protection against highly sophisticated cyber-attacks using multiple stage signature-less technologies.			
>Shall provide layered architecture that includes endpoint visibility, controls, prevention, detection, and remediation.			

>The proposed solution must include a web access control feature that allows administrators to permit or restrict web access for users or applications based on defined time schedules.			
>Shall provide process inspection that provides behavior-based real time detection; monitors all processes running in the operating system and if the process is deemed malicious, will terminate it.			
>Must have an integrated root cause analysis that highlights the attack vector, the attack entry point, and how the attack originated. Helps pinpoint the origin node of attack, highlighted in the incident page. The confidence score provides context for security events.			
Sandbox Analyzer			
>The proposed solution must provide an integrated sandbox analyzer to enhance targeted attack detection.			
>Shall provide pre-execution detection of advanced attacks by automatically sending files that require further analysis to cloud sandbox and taking remediation action based on the verdict.			
>The Sandbox module will be able to automatically send files to the Sandbox from the manufacturer's cloud where they can be "detonated" for an in-depth analysis.			
>The Sandbox module includes two analysis options: only monitoring or blocking. In monitoring mode, the user will be able to access the desired file, while in blocking mode, the user will be blocked from running the file until the Sandbox in the manufacturer's cloud gives the verdict.			
>The Sandbox module includes two types of remedial actions: default and safety. For the default action, it will be possible to set: only reporting, disinfection, deletion and quarantine. For the safety action, it will be possible to establish: deletion or quarantine.			
>The Sandbox module also includes the possibility of manually sending files to the Sandbox from the manufacturer's cloud. Thus, if the administrator suspects a file to be malicious, he can manually send it to the Sandbox to be „detonated" and find out the verdict. Administrator will be able to send several files at once, with the possibility to specify whether they will be „detonated" individually or all at the same time.			
>The Sandbox module can support " detonation" of the following types of files: Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archive), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE files (executable), PDF, PEF (executable), PIF (executable), RTF, SCR, URL (binary), VBE, VBS , WSF, WSH, WSH-VBS, XHTML.			
>The previously mentioned files will be able to be detected correctly even if they are included in archives of the type: 7z, ACE, ALZip, ARJ, Bzip2, cpio, Gzip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR , Unix Z, ZIP, ZIP (multivolume), ZOO, XZ.			
>The proposed Sandbox analyzer must be the same brand as the Endpoint Protection and manageable in the same console without the need for additional virtual/physical hardware and license.			
Endpoint Risk Analytics (ERA)			
>The proposed solution must provide integrated Endpoint Risk Analytics (ERA) that identifies, assesses, and remediates Windows endpoints weaknesses via security risk scans either on-demand or scheduled via policy, considering a vast number of indicators of risk.			
>Shall provide the ability to scan your network with certain indicators of risk and obtain an overview of network risk status via Risk Management dashboard, available from the Cloud Management Console.			
>Must have the ability to provide an overview of the company risk score and score evolution.			
>Must have the ability to provide an overview of statistics broken down into misconfigurations, vulnerable applications, and affected devices.			

>Must have the ability to provide a description of each indicator of risk and the recommended remediation actions.			
>Must have the ability to provide a Risk Management Dashboard that provides an overview of your network security and risk assessment information such as: " o Company Risk Score" " o Health Industry Modifier" " o Score Over Time" " o Top Misconfigurations " " o Top Vulnerable Apps " " o Top User Behavior Risks " " o Servers by Severity" " o Workstations by Severity" " o Top Devices at Risk " " o Top Users by Behaviors Risk "			
>Must have the ability to resolve certain security risks automatically from the Cloud Management Console, and view recommendations for endpoint exposure mitigation.			
>The proposed ERA must be the same brand as the proposed Endpoint Protection and manageable in the same console without the need for additional virtual/physical hardware and license.			
Endpoint Detection and Response (EDR)			
>The proposed solution must provide integrated Endpoint Detection and Response (EDR).			
>The proposed solution shall be a unified platform for preventative protection, post-breach detection, automated investigation, and response.			
>It shall offer pre and post compromises to attract visibility, alert triage, investigation, advanced search, and one-click resolution capabilities.			
>The EDR solution must include the collection of data and events related to "each workstation, bringing detailed maps of them as well as automatic actions and integration with the Sandbox module and the advanced security module.			
>Must have the ability to evaluate the typical activity of an endpoint from the perspective of its security according to MITRE ("baselining") attack techniques and can report any deviation from this behavior in the form of an incident.			
>The EDR module allows the filtering of incidents from the graphic interface depending on the time interval, based on a confidence score ("confidence score"), attack indicators, attack techniques (ATT&CK) respectively affected operating system as well as by IP, file name, station name.			
>The EDR module provides full visibility on the techniques, tactics, and procedures (TTPs) being used in active attacks while providing comprehensive search capabilities for specific indicators of compromise (IoCs), MITRE ATT&CK techniques and other artifacts to discover early-stage attacks.			
>The proposed EDR must be compatible with any pre-installed endpoint protection and will function as EDR (Report Only).			
>The proposed EDR must be the same brand as the Endpoint Protection and manageable in the same console without the need for additional virtual/physical hardware and license.			
Unified Management Console			
>The proposed solution must provide a single cloud-based centralized management console that manages the following security features: " o Endpoint Protection " " o Sandbox Analyzer " " o Endpoint Risk Analytics " " o Endpoint Detection and Response (EDR)"			
>The proposed solution must be a one-to-one license scheme and a transferable license wherein each endpoint device must have a dedicated license (1:1 ratio).			
>The solution should avoid kernel-mode deployment and utilize a lightweight agent instead.			
>The solution must have a built-in two-factor authentication (2FA) that works with authenticator apps (Google and Microsoft) and does not require additional			

hardware and license to set up.			
>Must have the capability to add, remove, arrange, configure, and customize the dashboard report, and does not limit the IT admin to a fixed dashboard.			
>Single policy template to manage the configuration of all the proposed security features.			
>Policy can be automatically changed depending on: " o IP or IP class of the station " " o The assigned gateway " " o Assigned DNS server " " o WINS assigned server " " o DNS suffix for DHCP connection " " o The client is/is not in the same network as the management " infrastructure (the workstation can implicitly resolve the hostname) " o Network type (LAN, wireless) "			
>Quarantined files can be stored for up to 180 days and can be remotely restored with a configurable location or deleted from the management console.			
>Shall provide the capability to retrieve and download quarantined files for further analysis to Sandbox Analyzer, from Windows, Linux, or macOS endpoints. The files available for download are restricted to 25MB each and have a maximum of 10 retrieved files per company.			
>Shall provide the capability to grant power user rights to access and modify the policy applied on the endpoints without the need to access the management console.			
>The administrator can customize installation packages including only desired modules: firewall, content control, device control, power user, and EDR sensor.			
>The proposed solution must allow downloading of full kit installer packages that don't require an internet connection upon installation.			
Third Party Rating, Evaluation, Compatibility, and other requirements			
>The solution should be able to integrate with Microsoft Active Directory.			
>The solution must be in the Leaders Part of Forrester Wave™: Endpoint Security provider, Q4 2023 or later.			
>The solution participated in the annual MITRE ATT&CK Evaluations 2022 or later for EDR conducted by MITRE Ingenuity ATT&CK Evaluations.			
>The solution must be a visionary player in the recent Gartner Magic Quadrant of 2024 for EPP.			
>The vendor/provider should provide proof of at least (2) certified technical engineers with expertise in the endpoint security solution.			
Technical Support and Product Training			
>The supplier/vendor must conduct Admin and End user product training/technology transfer with issuance of individual training certificates and training materials for each of the participants.			
>The supplier/vendor shall provide/render 10-hours remote installation and implementation services during office hours (Monday-Thursday) excluding holidays with at least one (1) assigned Technical Engineer.			
>Shall provide/render twenty-four hours a day, seven days a week (24x7) technical support service that can be delivered in the form of Viber call or message, electronic mail and/or on-site support.			
>The supplier/vendor shall resolve the issue raised by the end user within eight (8) hours after it was reported.			
Delivery Requirement:			
>Delivery of licenses: 20 days			

FINANCIAL OFFER:

Please quote your **best offer** for the items below. Please do not leave any blank items. Indicate **"0"** if item being offered is for free.

Subscription of Advance Endpoint Security Solution for the Philippine Sports Commission			
Approved Budget for Contract	Quantity in Set (A)	Offered Price per Set (B)	Your Total Offered Quotation (A x B)
Item 1 **Subscription of Advance Endpoint Security Solution (12 Months Subscription)** Nine Hundred Ninety Thousand and One Hundred Ninety Two Pesos (PhP 990,192.00)	421 licenses		In Figures: _____
Grand Total: **Nine Hundred Ninety Thousand and One Hundred Ninety Two Pesos (PhP 990,192.00)**	**Total Offered Quotation**		In Words: _____ _____ _____ In Figures: _____

TERMS AND CONDITIONS:

1) Bidders shall provide correct and accurate information required in this form.
2) Price quotation/s must be valid for a period of thirty (30) calendar days from the date of submission.
3) Price quotation/s, to be denominated in the Philippine Peso shall include all taxes, duties and/or levies payable.
4) Quotations exceeding the Approved Budget for the Contract shall be rejected.
5) Award of contract shall be made to the lowest quotation (for goods and infrastructure) or, the highest rated offer (for consulting services) which complies with the minimum technical specifications and other terms and conditions stated herein.
6) Any interlineations, erasures or overwriting shall be valid only if they are signed or initiated by you or any of your duly authorized representative/s.
7) The item/s shall be delivered according to the requirements specified in the Technical Specifications.
8) The PSC shall have the right to inspect and/or to test the goods to confirm their conformity to the technical specifications.
9) In case of two or more bidders are determined to have submitted the Lowest Calculated Quotation/Lowest Calculated and Responsive Quotation, the PSC shall adopt and employ "draw lots" as the tie-breaking method to finally determine the single winning provider in accordance with GPPB Circular 06-2005.
10) Payment shall be made after delivery and upon the submission of the required supporting documents, i.e., Order Slip and/or Billing statement, by the supplier, contractor or consultant.
11) Liquidated damages equivalent to one tenth of one percent (0.1%) of the value of the goods not delivered within the prescribed delivery period shall be imposed per day of delay. The PSC shall rescind the contract once the cumulative amount of liquidated damages reaches ten percent (10%) of the amount of the contract, without prejudice to other courses of action and remedies open to it.

_____
Signature over Printed Name

_____
Position/Designation

_____
Office Telephone/Fax/Mobile Nos.

_____
E-Mail Address/es