Republic of the Philippines
Office of the Solicitor General
134 Amorsolo St. Legaspi Village, Makati City

Technical Working Group for
Information and Communications Technology

TERMS OF REFERENCE

1-YEAR LICENSE OF ENDPOINT PROTECTION (ANTI-VIRUS)

Background:

The Office of the Solicitor General (OSG) aims to enhance cybersecurity by expanding its Endpoint Protection (Antivirus) subscription. This initiative responds to the evolving threat landscape, particularly the rising frequency and sophistication of endpoint attacks. By strengthening its endpoint security, the OSG seeks to safeguard its systems from viruses, malware, and other cyber threats.

This move reflects the OSG's commitment to maintaining robust cybersecurity measures considering growing digital vulnerabilities. Enhancing endpoint protection will help ensure the security and integrity of sensitive government data and reduce the risk of disruptions caused by malicious attacks.

Objective:

The objective is to implement a comprehensive endpoint security solution that offers real-time protection against a wide range of cyber threats, including malware, ransomware, and advanced persistent threats. This solution will proactively monitor and defend all endpoint devices across the network, ensuring continuous protection through advanced threat detection and automated responses to potential risks.

Additionally, the solution aims to enhance visibility and control over endpoint activities, enabling IT administrators to identify vulnerabilities and address security incidents swiftly. Integrating advanced behavioral analytics and threat intelligence strengthens the organization's overall cybersecurity posture, ensuring minimal disruption to operations while protecting sensitive data.

Terms:

1. *Scope.* – Supply and delivery of eight hundred (850) 1-Year License of Endpoint Protection (Anti-Virus)

2. *ABC.* - The Approved Budget for the Contract (ABC) is **Two Million Pesos (₱2,000,000.00)**, inclusive of all government taxes, charges, and other standard fees.

ICT SUBSCRIPTION			
ITEM	**QTY**	**UNIT COST**	**TOTAL**
(850) 1-Year License of Endpoint Protection (Anti-Virus)	1	2,000,000.00	2,000,000.00
		TOTAL	**₱ 2,000,000.00**

3. *Deliverables and Training*:

   a. Eight hundred fifty (850) licenses of endpoint protection (antivirus) solutions valid for a one-year (1 year) subscription from the date of installation and deployment.

   b. Provide a technical person to assist in uninstalling OSG's existing endpoint protection solution and installing the proposed solution.

   c. All items should be delivered within 30 days of receipt of the Notice to Proceed.

   d. Provide training to CMS staff in administering the proposed endpoint protection solution. Training materials, product guides, and documentation should be available online. Must be done during business hours and the course outline should be presented.

   e. Training must begin upon deployment within ten (10) days of solution delivery and must be coordinated with CMS. The CMS will provide certification for delivery and training completion.

4. *Warranty* - The principal of the Antivirus Solution warrants maintaining the usability of the antivirus product during the subscription period through regular updates and upgrades substantially under the documentation of the solution provided.

5. *Guarantee and Schedule of Payment.* - To guarantee the performance by the winning bidder of its obligations under the contract, it shall post a performance security before the signing of the contract. The performance security shall be in an amount not less than the required percentage of the total contract price in any of the following forms and by the following schedule:

Form of Performance Security	Amount of Performance Security (Not less than the required % of the Total Contract Price)	Statement of Compliance
a) Cash or cashier's/ manager's check issued by a Universal of Commercial Bank.	5%	
b) Bank draft/ guarantee or irrevocable letter of credit issued by a Universal or Commercial Bank; *however,* it shall be confirmed or authenticated by a Universal or Commercial Bank if issued by a foreign bank.	5%	
c) Surety bond callable upon demand issued by a surety or insurance company duly certified by the Insurance Commission as authorized to issue such security.	30%	

TERMS OF PAYMENT	Statement of Compliance
Supplier agrees to be paid based on a progressive billing scheme as follows:	
• Within thirty (30) days from completion of the delivery and issuance of the Inspection and Acceptance Report by the OSG and submission of all other required documents - 95% of the contract price. • One (1) year from the issuance of the Inspection and Acceptance Report by the OSG - 5% of the contract price.	

All bid prices shall be considered as fixed prices, and therefore not subject to price escalation during contract implementation.

6. *Qualifications of the Supplier*:

   a. The bidder/supplier should be duly authorized to provide, sell, configure, and support the endpoint protection product it intends to offer.

   b. The bidder/supplier must have satisfactorily completed, within the last three years from the date of submission and

receipt of at least one (1) single contract of a similar nature amounting to at least fifty percent (25%) of the ABC.

For this purpose, the purchase of cybersecurity or antivirus shall be referred to as a similar contract.

c. The bidder/supplier shall submit a valid and current Certificate of Distributorship/Dealership/ Resellers of the product being offered, issued by the principal or manufacturer of the product (if the bidder is not the manufacturer). If not issued by the manufacturer, must also submit a certification/document linking the bidder to the manufacturer.

d. The bidder/supplier must maintain its status as an authorized distributor, reseller, or partnership with the manufacturer/principal for the duration of the contract. Failure to maintain such status is a ground for the OSG to terminate the said contract.

e. The bidder shall have at least one (1) personnel to support the solution offered with a manufacturer certification. The bidder must provide a certificate as part of the technical requirements.

f. The principal of the offered solution must have a local office and a local agent in the Philippines to ensure compliance with local laws and regulations. Additionally, direct local engineers should be employed to oversee the implementation of technical services, ensuring adherence to local standards and project specifications.

g. The financial proposal shall include all costs necessary for the supplier to fulfill its obligation to deliver and deploy endpoint protection (software, hardware, etc.).

7. Applicable provisions of the Government Procurement Reform Act (RA No. 9184) and its Revised Implementing Rules and Regulations (RIRR) shall form part of the Terms of Reference.

==========

Technical Specifications:

ITEM	SPECIFICATIONS	COMPLIANCE
Scope of Protection	– The solution must be an Endpoint Protection Platform (EPP) that integrates Next Generation Anti-Virus (NGAV), Endpoint Detection and Response (EDR), and endpoint management capabilities into a single solution	
	– The solution must provide endpoint protection across various devices, including desktops, laptops, and servers, to defend against advanced persistent threats, ransomware, malware, and fileless attacks.	
Endpoint Management Platform	– The solution must be capable of providing both local and cloud management platform	
	– The solution should support collecting endpoint information of OS, service ports, users, applications, databases applications, websites, web frameworks, web services, and web applications to help you learn the status of your server assets and improve asset management efficiency.	
	– The solution should have centralized management and monitoring update software. It should allow for slave servers, tools for distributing both the client agents and signature database updates to other clients, distribution of all agents in a single action, and monitoring of the agent's health.	
	– The solution should have the capability to update databases of signatures for malicious programs and attacks. It should use the same mechanism to distribute signatures, updates, firewall policies, and engine updates	
	– The solution should support unmanaged endpoints detected by other same-segment endpoints.	
	– The solution should support P2P installation and upgrade; an endpoint with the agent deployed or upgraded can distribute resource packages to other	

	endpoints in the subnet for agent deployment and upgrade, significantly improving the efficiency of deploying and upgrading the agent on endpoints.	
	– The solution should support identifying the development environment, significantly improving security, reducing computer lagging issues, and improving efficiency.	
	– The solution should allow the administrator to configure flexible scanning options to prioritize endpoints' CPU and disk utilization over scanning	
Detection and Protection	– The solution must include but is not limited to Protection software for Windows workstations, MacOS, Linux workstations, Oracle, Active Directory,	
	– The solution must protect end-of-support (legacy) operating systems, including XP, WIN7, Windows Server 2003, Windows Server 2008, etc.	
	– The solution should allow for simulation of unknown code before execution to determine malicious intent without user intervention	
	– The solution should have a Heuristic analyzer that allows the identification and blocking of previously unknown malware more efficiently, including zero-day outbreaks	
	– The solution should have AI capabilities that allow identification and blocking of previously unknown malware based on malware family classification	
	– The solution should be capable of checking and disinfection files in archives using the RAR, ARJ, ZIP, CAB, LHA, JAR, and ICE formats up to 16 layers.	
	– The solution should provide a forced scan channel for stubborn viruses	
	– The solution should have application control that prevents applications from performing actions that may be dangerous for the system.	
	– The solution should support advanced threat detection to detect hot threats (ransomware, crypto mining, etc.) and	

	new attack methods such as fileless attacks and in-memory attacks. This function helps you categorize attacks by comparing the characteristics of the collected behavior data (process operation, network connection, module loading, file operation, registry modification, etc.) with the characteristics of advanced threat attack techniques defined by the ATT&CK framework.	
	– The solution should support honeypot (bait files) to detect ransomware	
	– The solution should support detection and blocking of all types of ransomware execution through AI-based detection engine(s).	
	– The solution should identify high-confidence events such as phishing and web intrusion attacks, tag security events with phishing and web intrusion, and provide users with greater context of the events.	
	– The solution should support blocking specific applications or alerting when specified applications are executed on the endpoints. The list of applications should be configurable by the administrator.	
	– The solution should support web/URL filtering to block endpoints from accessing specific websites and URL	
	– The solution should support USB Control for Windows and macOS Operating System	
	– The solution must identify and block/alert on lateral movement (SMB relay, pass the hash).	
	– The solution should provide a secondary authentication capability for the RDP session	
	– The solution should have real-time ransomware protection to detect and block encryption of endpoints and shared folders	
	– The solution should have capabilities to allow administrators to isolate endpoints from the network, leaving only an active	

	connection with the Manager, with minimal effort from the management console	
	– The solution should provide anti-brute force for SMB, RDP session	
	– The solution should detect and block real-time anti-proxy/VPN/proxy avoidance applications.	
	– The solution should have vulnerability scanning for computers in the network and the ability to provide reports on detected software vulnerabilities and rootkits. It should be able to run scheduled, on-demand, and real time on access scans	
	– The solution should have Integrated patch management functionality: centralized discovery and remote installation of OS and third-party detections and updates	
	– The solution should support endpoint CPU restrictions to make scanning more lightweight, which can reduce performance impacts on legacy systems, virtual desktops, and overloaded systems.	
	– The solution should provide a list of system resources that are detected to have possible malware presence, e.g., host files and registry.	
	– The solution should accommodate resident antivirus monitoring.	
	– The solution should have tasks launched by schedule and/or just after loading the operating system.	
Threat Intelligence	– **Threat Intelligence Integration**: Real-time integration with global threat intelligence sources to provide up-to-date protection against emerging threats.	
	– The solution should have data feeds to inform the business about risks and implications associated with cyber threats and defend against attacks even before they are launched. They may include	

	Malicious Hash feeds, Whitelisting Data Feeds, and Botnet C&C URL Feeds.	
	– The solution should require each Data Feed to output actionable context, such as threat names, timestamps, geolocation, resolved IP addresses of infected web resources, etc.	
	– The solution should have threat intelligence generated in real-time	
	– The solution should have intelligence services that allow the detection of malware in all types of traffic, such as web, Email, P2P, Instant Messaging, etc.	
	– The solution should have the capability to conduct intricate searches into threat indicators	
	– The solution should have Advanced Persistent Threat Intelligence	
	– The solution should have an Identification of notable threats for different states and different locations or countries	
Endpoint Management Functionalities	– The solution should support easy searching and exporting asset inventories across all workstation and server assets, such as software and ports, processes, system information, and more.	
	– The solution should support remote uninstallation of applications.	
	– The solution should allow the administrator to configure a list of software and the allowable number of licenses that can run in their environment. Any instance of the software running exceeding the allowable number of licenses will be alerted to the administrator.	
Certification and Recognition	– To ensure the maturity of the solution, the vendor/principal must have CMMI L5 Certifications and the following ISO Certifications: a) ISO 9001 Certification	

	b) ISO 20001 Certification c) ISO 27001 Certification	
	– Must pass AV-Test Top Product Award with Perfect Scores for at least the end (December) of 2023.	
Support Service Requirement	The bidder must provide the following:	
	* Unlimited corrective maintenance/ repair services within the warranty period	
	* Twenty (24) hours by seven (7) days (Monday to Friday) technical support and must meet the following response and resolution time:	
	> Within one (1) hour for phone or email support	
	> Within two (2) hours of response time for on-site support	
	> Root cause analysis for all support cases filed.	
	* The bidder must provide full documentation for the Activity Plan on the installation of patches and upgrades and Root Cause Analysis of incidents encountered.	
	* The bidder must provide onsite support for installing and deploying software patches and version upgrades.	
	* The bidder must provide a procedure for support and problem escalation.	
	* Submission of Activity/Service Report within 5 calendar days	

==========

Technical Working Group for ICT Subscriptions

SSS JOEL N. VILLASERAN

DIR IV EDUARDO ALEJANDRO O. SANTOS

ITO III JAYVIE NEIL MALICK S. MALICDEM

ITO II CEDRIC S. DELA CRUZ

SAO JOY Y. CHUA

CMT III JESUS NIÑO CHUA

AO IV RAY CHARLIE V. ALEGRE

Approved/Disapproved:

MENARDO I. GUEVARRA
Solicitor General

Certified Funds Available:

BERNADETTE M. LIM
Dir IV - FMS