



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) is seeking to replace its Endpoint Protection (Antivirus) subscription for the fiscal year 2023 for endpoint security and protection against computer viruses and malware attacks to cope with the changing threat of endpoint attacks.

Objective:

To procure and implement comprehensive endpoint protection solutions for the workstations of the OSG in order to safeguard against cybersecurity threats, ensure data integrity, and maintain uninterrupted business operations.

This project involves purchasing licenses for the Endpoint Protection (Anti-Virus) subscription to be deployed to the computers and servers of the office.

Terms:

1. *Scope.* - Supply and delivery of eight hundred (800) 1-Year License of Endpoint Protection (Anti-Virus)
2. *ABC.* - The Approved Budget for the Contract (ABC) is **One Million and Five Hundred Thousand Pesos (₱1,500,000.00)**, inclusive of all government taxes, charges and other standard fees.

ICT SUBSCRIPTION			
ITEM	QTY	UNIT COST	TOTAL
(800) 1-Year License of Endpoint Protection (Anti-Virus)	1	1,500,000.00	1,500,000.00
TOTAL			₱ 1,500,000.00

3. *Deliverables:*
 - a. Eight hundred (800) licenses of endpoint protection 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. Provide technical training to CMS staff in administering the proposed endpoint protection solution.

4. *Delivery:*

- a. All items should be delivered within 30 days of receipt of the Notice to Proceed.
- b. Provide training covering essential items for correct use and day-to-day administration.
- c. Training materials, product guides, and documentation should be available online.
- d. Must be done during business hours
- e. The course outline should be presented.
- f. Training must begin upon deployment within ten days of solution delivery and must be coordinated with CMS. The CMS will provide certification for delivery and training completion.

5. *Limited Warranty* - The Antivirus Solution will maintain the usability of the Antivirus Product during the Subscription Period through regular updates and upgrades substantially in accordance with the documentation of the solution provided.

6. *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 in accordance with 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; <i>however</i> , 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:	
<ul style="list-style-type: none"> • 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.

7. *Qualifications of the Supplier:*

- a. The supplier should be duly authorized to provide, sell, configure, and support the endpoint protection product it intends to offer.
- b. The bidder must have completed, within the last three (3) years from the date of submission and receipt of at least one (1) single contract of similar nature amounting to at least fifty percent (50%) of the ABC; or the prospective bidder should have completed at least two (2) similar contracts, and the aggregate contract amounts should be equivalent to at least fifty percent (50%) of the ABC, and

=====

the largest of these similar contracts must be equivalent to at least half of the fifty percent (50%) of the ABC as required.

- c. The bidder 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, they must also submit a certification/document linking the bidder to the manufacturer.
- d. The bidder shall have at least one (1) personnel to support the solution offered with a manufacturer certification. Must provide a certificate as part of technical requirements.
- e. During contract implementation, the bidder/supplier must ensure that it remains an authorized distributor, reseller, or partner to maintain said License Software. Suppose the bidder/supplier cannot maintain its distributor, reseller, or partnership agreement with the Manufacturer/Principal. In that case, this may serve as grounds/reason for the termination of its contract with OSG.
- f. The supplier must be able to escalate product technical issues directly with the endpoint protection service provider.
- g. All costs necessary for the supplier to fulfill its obligation to deliver and deploy endpoint protection (software, hardware, etc.) shall be included in the financial proposal.

8. 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
Specific Requirements for Endpoint Protection (Anti-Virus)		
Anti-malware	- The solution should have protection based on signature scanning and heuristic analysis against viruses, worms, Trojans, spyware, adware, keyloggers, rootkits, and other types of malicious software.	
	- Should have employed the traditional scanning method where scanned content is matched against the signature database	
	- With a separate layer of protection against brand new, undocumented threats using heuristic algorithms to detect malware based on behavioral characteristics	

=====

	<ul style="list-style-type: none"> - Able to automatically set the scanning engines when creating security agent packages according to the endpoint's configuration 	
	<p>Customizable scan engines, being able to choose between several scanning technologies:</p> <ol style="list-style-type: none"> 1. Local Scan 2. Hybrid Scan with light Engines 3. Central Scan in Public or Private Cloud 4. Central Scan (Public or Private Cloud scanning with Security Server) with fallback* on Local Scan (Full Engines) <ul style="list-style-type: none"> - Central Scan (Public or Private Cloud scanning with Security Server) with fallback* on Hybrid Scan (Public Cloud with Light Engines) 	
	<ul style="list-style-type: none"> - Should be able to support dual-engine scanning where the fallback engine will be used if the first engine is unavailable. 	
	<ul style="list-style-type: none"> - The solutions should be able to auto-quarantine or autodelete identified malware without end-user interaction. 	
Advance Threat Control	<ul style="list-style-type: none"> - Can continuously monitor running processes and grade suspicious behaviors such as attempts to: disguise the type of process, execute code in another process's space (hijack process memory for privilege escalation), replicate, drop files, hide from process enumeration applications, etc. Each suspicious behavior raises the process rating. When a threshold is reached, an alarm is triggered. 	
	<ul style="list-style-type: none"> - Designed to detect advanced attacks and suspicious activities in the pre-execution stage. 	
	<ul style="list-style-type: none"> - Should contain and implement machine learning models and stealth attack detection technology against threats such as zero-day attacks, advanced persistent threats (APT), obfuscated malware, fileless attacks (misuse of PowerShell, Windows Management Instrumentation, etc.), credential stealing, targeted attacks, custom malware, script-based attacks, exploits, hacking tools, suspicious network traffic, potentially unwanted applications (PUA), ransomware. 	
Anti-exploit	<ul style="list-style-type: none"> - Catches the latest exploits in real-time and mitigates memory corruption vulnerabilities that can evade other security solutions. 	
	<ul style="list-style-type: none"> - Has a proactive technology that stops zero-day attacks carried out through evasive exploits 	
	<ul style="list-style-type: none"> - Powered by Machine Learning technology 	

=====

	<ul style="list-style-type: none"> - Detects exploit methods and protects the memory space of browsers, document viewers, media players, and office applications. 	
Firewall	<ul style="list-style-type: none"> - Controls applications' access to the network and to the Internet. 	
	<ul style="list-style-type: none"> - Access is automatically allowed for a comprehensive database of known, legitimate applications. 	
	<ul style="list-style-type: none"> - The firewall can protect the system against port scans, restrict internet connection sharing (ICS) and warn when new nodes join a Wi-Fi connection. 	
Content Control	<ul style="list-style-type: none"> - Can enforce company policies for allowed traffic, web access, data protection, and application control. 	
	<ul style="list-style-type: none"> - Administrators can define traffic scan options and exclusions, schedule web access while blocking or allowing specific web categories or URLs, 	
	<ul style="list-style-type: none"> - Configurable data protection rules can define permissions for the use of specific applications. 	
Network attack defense	<ul style="list-style-type: none"> - Has a technology that focuses on detecting network attacks designed to gain access to endpoints through specific techniques, such as brute-force attacks, network exploits, password stealers, drive-by-download infection vectors, bots, and Trojans. 	
Device Control	<ul style="list-style-type: none"> - Allows to prevent sensitive data leakage and malware infections via external devices attached to endpoints by applying blocking rules and exceptions via policy to a vast range of device types (such as USB flash drives, Bluetooth devices, CD/DVD players, storage devices, etc.). 	
Encryption	<ul style="list-style-type: none"> - This protection layer allows you to provide full disk encryption on endpoints. 	
	<ul style="list-style-type: none"> - Can encrypt and decrypt boot and non-boot volumes 	
	<ul style="list-style-type: none"> - Can store the recovery keys needed to unlock volumes when the users forget their passwords. 	
	<ul style="list-style-type: none"> - Utilize existing Windows BitLocker and MAC OS FileVault native encryption with centralized deployment and management 	
Security for Exchange	<ul style="list-style-type: none"> - Security for Exchange provides antimalware, antispam, anti-phishing, attachment, and content filtering seamlessly integrated with the Microsoft Exchange Server to ensure a secure 	

=====

	<p>messaging and collaboration environment and increase productivity.</p>	
	<ul style="list-style-type: none"> - It protects Exchange users against the latest, most sophisticated malware and against attempts to steal users' confidential and valuable data. 	
Application Control	<ul style="list-style-type: none"> - The Application Control module prevents malware and zero-day attacks and enhances security without impacting productivity. 	
	<ul style="list-style-type: none"> - Enforces flexible application whitelisting policies that identify and prevent the installation and execution of unwanted, untrusted, or malicious applications. 	
	<ul style="list-style-type: none"> - Supports both "Default Deny" and "Blacklisting" 	
Sandbox Analyzer	<ul style="list-style-type: none"> - Sandbox Analyzer that provides a powerful layer of protection against advanced threats by performing automatic, in-depth analysis of suspicious files not signed by antimalware engines yet. 	
	<ul style="list-style-type: none"> - The sandbox employs an extensive set of technologies to execute payloads in a contained virtual environment hosted by a solution or deployed locally, analyze their behavior, and report any subtle system changes indicative of malicious intent. 	
	<ul style="list-style-type: none"> - Sandbox Analyzer uses sensors to detonate content from managed endpoints, network traffic streams, centralized quarantine, and ICAP servers. 	
	<ul style="list-style-type: none"> - Automatic submission of suspicious files from endpoints to a cloud-based sandbox for detonation and behavioral analysis 	
	<ul style="list-style-type: none"> - Allows manual detonation of suspicious files in the Sandbox Analyzer 	
Hypervisor Memory Introspection	<ul style="list-style-type: none"> - HVI protects data centers with a high density of virtual machines against advanced and sophisticated threats that signature-based engines cannot defeat. 	
	<ul style="list-style-type: none"> - It enforces strong isolation, ensuring real-time detection of the attacks, blocking them as they happen, and immediately removing the threats. 	
	<ul style="list-style-type: none"> - HVI has intimate knowledge of both user-mode and kernel-mode in-guest memory. The result is that HVI has complete insight into guest memory and, therefore, full context. 	

=====

	<ul style="list-style-type: none"> - HVI identifies attack techniques rather than attack patterns. This way, the technology can identify, report, and prevent common exploitation techniques. 	
	<ul style="list-style-type: none"> - The kernel is protected against rootkit hooking techniques used during the attack kill chain to provide stealth. 	
	<ul style="list-style-type: none"> - User-mode processes are protected against code injection, function detouring, and code execution from stack or heap. 	
Network Traffic Security Analysis	<ul style="list-style-type: none"> - A network security solution that analyzes IPFIX traffic streams for the presence of malicious behavior and malware. 	
	<ul style="list-style-type: none"> - Prevent malware infections by inspecting inbound traffic (via sandbox, firewalls, antivirus, and so on). 	
	<ul style="list-style-type: none"> - Focuses on monitoring outbound network traffic for malicious behavior. 	
Security for Storage	<ul style="list-style-type: none"> - Real-time protection for leading file-sharing and network-storage systems. 	
	<ul style="list-style-type: none"> - System and threat-detection algorithm upgrades happen automatically or without requiring any effort from an administrator or creating disruptions for end-users. 	
	<ul style="list-style-type: none"> - Provides antimalware services to Network-Attached Storage (NAS) devices and file-sharing systems compliant with the Internet Content Adaptation Protocol (ICAP, as defined in RFC 3507). 	
Security for mobile	<ul style="list-style-type: none"> - Unifies enterprise-wide security with management and compliance control of iPhone, iPad, and Android devices by providing reliable software and update distribution via Apple or Android marketplaces. 	
	<ul style="list-style-type: none"> - Enforces usage policies consistently on all portable devices. Security features include screen lock, authentication control, device location, remote wipe, detection of rooted or jailbroken devices, and security profiles. 	
	<ul style="list-style-type: none"> - On Android devices, the security level is enhanced with real-time scanning and removable media encryption. As a result, mobile devices are controlled, and sensitive business information residing on them is protected. 	
Incident Reporting	<ul style="list-style-type: none"> - Creates an incident map that visualizes events related to a suspicious process to help triage incidents 	

=====

Patch Management	- Fully integrated patch management keeps operating systems and software applications up to date and provides a comprehensive view of the patch status for managed endpoints.	
	- Features include on-demand / scheduled patch scanning, automatic/manual patching, or missing patch reporting.	
	- Support with different vendors and products patches	
Technology	- Allows the solution to scale with ease and secure any number of systems. It can be configured using multiple virtual appliances and instances of specific roles (Database, Communication Server, Update Server, and Web Console) to ensure reliability and scalability.	
	- It can be imported to run on any virtualization platform, including VMware, Citrix, Microsoft Hyper-V, Nutanix Prism, and Microsoft Azure.	
	- It can be managed from a single point of management. This provides easier management and access to overall security posture, global security threats, and control over all security modules protecting virtual or physical desktops, servers, and mobile devices.	
	Dynamic Machine Learning: <ul style="list-style-type: none"> • Algorithms trained in URL filtering and file analysis on 500M endpoint-sensors. • Trillions of samples deliver top efficacy with low false positives. 	
OS Support	- Support different platforms, including Windows, Mac, Linux, Windows Server, Android, and iOS.	
Integration	Has seamless integration with the existing network management system of OSG. -	
	- Control Center can be integrated with the existing system management and monitoring systems to make it simple to apply protection to unmanaged workstations automatically, servers, or mobile devices that appear on the Microsoft Active Directory, VMware vCenter, Nutanix Prism Element or Citrix XenServer, or that are detected in the network.	
Certification and Recognition	The solution must have any two (2) certifications of the following: <ul style="list-style-type: none"> • SOC 2 Type Compliant • ISO 9001 Quality Management Systems - ISO 27001 Information Security Management	

=====


	<p>Must have been recognized and awarded by the following:</p> <ul style="list-style-type: none"> • Forrester • Radicati Group • AV-TEST Institute • AV-Comparatives • CRN Tech Innovator Award • MRG Effitas <p>MITRE ATT&CK Evaluation</p>	
Deployment	Deploy Agent Remotely thru Active Directory	
	Deploy Agent via URL Link and can be distributed thru corporate email notification.	
	Deploy Agent using 3 rd party application/tool.	
	Deploy Agent thru distribution of copies using any medium (like USB drive, CD, etc.)	
	Deploy Agent through sharing the downloaded file in the corporate on-premises repository to avoid using corporate internet bandwidth.	

=====

Technical Working Group for ICT Subscriptions



DIR IV EDUARDO ALEJANDRO O. SANTOS



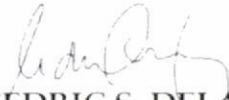
DIR IV EDITHA R. BUENDIA



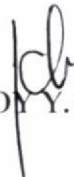
SS II OMAR T. GABRIELES

ASII MIGUEL MARTIN A. BUENAVENTURA
(RESIGNED)

ASII JONATHAN A. PABILLORE
(STUDY LEAVE)



ITO II CEDRIC S. DELA CRUZ



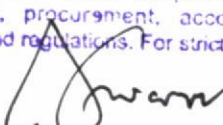
SAO JOY Y. CHUA

CMT III JESUS NIÑO CHUA



AO IV RAY CHARLIE V. ALEGRE

APPROVED
It is understood that the foregoing shall be subject to availability of funds and strict compliance with the pertinent budgeting, procurement, accounting and auditing laws, rules and regulations. For strict compliance.



MENARDO I. GUEVARRA
Solicitor General
NOV 22 2023

Approved/Disapproved:

MENARDO I. GUEVARRA
Solicitor General

Certified Funds Available:

BERNADETTE M. LIM
Dir IV - FMS