Republic of the Philippines
NATIONAL PRIVACY COMMISSION

REQUEST FOR QUOTATION

PROCUREMENT OF ANTI-VIRUS

08 December 2020

NOTICE TO ALL PROVIDERS/SUPPLIERS:

The National Privacy Commission intends to procure **supply, delivery, configuration, and installation of antivirus/endpoint security subscription.**

As such, providers or suppliers of known qualifications are hereby invited to submit their quotations/price proposals signed by your authorized representative not later than **4:00 P.M., 14 December 2020.**

The service providers/suppliers must also submit the following requirements:

1. Mayor's Permit issued by the city or municipality where the principal place of business of the prospective bidder is located;
2. PhilGEPS Registration Number;
3. Notarized Omnibus Sworn Statement; and
4. Manifestation of compliance to the attached technical specification signed by your authorized representative.

Please submit your quotation together with the required documents via e-mail to bacsecretariat@privacy.gov.ph or via mail or courier in a sealed envelope to:

5th Floor, Ang Kiukok Hall,
PICC Delegation Building, PICC Complex,
Roxas Boulevard Manila 1307

Attention to: **ATTY. KRISHNA AIRA TANA-CAGUIA**
BAC Secretariat Head

Digitally signed by Tana-Caguia Krishna Aira Angeles
Date: 2020.12.08 20:17:21 +08'00'

ATTY. KRISHNA AIRA TANA-CAGUIA
BAC Secretariat Head
National Privacy Commission
(02) 8234-2228 loc. 127

Republic of the Philippines
NATIONAL PRIVACY COMMISSION

TECHNICAL SPECIFICATION

Item	Unit	QTY	Description/Specifications	Approved Budget of the Contract (Php 500,000.00)		Compliance (Manifest your compliance by writing "COMPLY" in every item)
				Unit Price	Total	
	lot	1	***NOTE: Please refer to the attached Terms of Reference for:*** 1. Technical Specifications 2. Service Level Agreement 3. Instructions to Bidders 4. Evaluation Process 5. Payment Terms			
			TOTAL			

Instruction to bidders.

I. All prices shall be VAT inclusive.
II. All quotations shall be written with the company's letterhead.
III. Compliance must be stated by writing "Comply" to each requirement mentioned above.
IV. Present the original Mayor's Permit and submit original Omnibus Sworn Statement upon the scheduled signing of Notice of Award for inspection.
V. Acknowledgement of the Notice of Award shall be within five (5) days from its issuance.
VI. Payment shall be prepared through Advice to Debit Account upon completion of deliveries and receipt of the supplier's Statement of Account, subject to deduction of applicable taxes monthly.

CONFORME: _____
(Name of Supplier/Provider/Date)

BY: _____
(Name/Position/Signature of Representative/Date)

Republic of the Philippines
NATIONAL PRIVACY COMMISSION

ANTI-VIRUS

(SUPPLY, DELIVERY, CONFIGURATION & INSTALLATION OF ANTIVIRUS/ENDPOINT SECURITY SUBSCRIPTION FOR THE NATIONAL PRIVACY COMMISSION)

Republic of the Philippines
NATIONAL PRIVACY COMMISSION

TABLE OF CONTENTS

SUPPLY, DELIVERY, CONFIGURATION & INSTALLATION OF ANTIVIRUS/ENDPOINT SUBSCRIPTION FOR THENATIONAL PRIVACY COMMISSION 1

I. BACKGROUND 3

II. PURPOSE OF THE PROCUREMENT 3

III. TECHNICAL SPECIFICATIONS 3

IV. MODE OF PROCUREMENT 7

V. NATURE OF PROCUREMENT 7

VI. SOURCE OF FUNDS AND APPROVED BUDGET FOR THE CONTRACT (ABC) 7

VII. INSTRUCTIONS TO BIDDERS 7

VIII. EVALUATION PROCESS 8

IX. PAYMENT TERMS 8

Republic of the Philippines
NATIONAL PRIVACY COMMISSION

TERMS OF REFERENCE

I. BACKGROUND

The National Privacy Commission (NPC) is tasked to inform and educate the public about data privacy, data protection, and fair information rights and responsibilities, as provided in Section 9.c of the Implementing Rules and Regulations of R.A. 10173 or the Data Privacy Act of 2012. In this regard, the Interim Management Information System Unit (IMISU) proposes the subscription to an Anti-Virus and End Point Security subscription to secure and protect NPC Endpoint Devices like Laptop/Desktop Workstation and Servers. The subscription will help prevent malicious traffic and cyberattacks targeting the NPC employees and End Point Devices of the Commission.

II. PURPOSE OF THE PROCUREMENT

To increase the security posture of the Commission, an enterprise-level anti-virus and endpoint security must be properly configured, installed and maintained among Commission-issued computers and endpoint devices in the data center. This shall act as endpoint security to protect all endpoints like servers, desktops, laptops, smartphones and other IoT devices from cyberattacks.

With the current (Bring Your Own Device) BYOD practice of NPC employees who do not have NPC-issued computers and the ever-increasing incidences of information security threats, an antivirus or endpoint security has become a crucial requirement for the NPC. This is especially true for employees connecting to non-NPC networks using their laptops and mobile devices during field work, telecommuting and other alternative work arrangements.

III. TECHNICAL SPECIFICATIONS

LOT	FEATURES AND CAPABILITIES
1 lot	Protects NPC ICT endpoints infrastructure daily (at least two hundred fifty (250) end user licenses for one year
	Able to provide at least 99.5% Protection Rate and less than 10 False Alarms in Real-World Protection Test (March-June 2020) (see https://www.av-comparatives.org/tests/business-security-test-2020-march-june/)

	Available ON CLOUD or ON-PREMISE with Management Console
	With multi-stage signature-less technologies able to detect and prevent computer viruses and malwares in real time.
	Able to provide the latest virus definition and constant updates from the manufacturer and capable of manual and automatic updates of virus definition on premise server and from the internet
	Able to use machine learning techniques use well-trained machine models and algorithms to predict and block advanced attacks.
	Able to continuously monitor all processes that are running in the operating system this is done through monitoring of suspicious activities or anomalous process behavior, 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 and more. It takes appropriate remediation actions, including process termination and undoing changes the process made.
	Able to tackle advanced, evasive exploits that targeted attacks rely on to penetrate an infrastructure and prevent exploits and protects the memory and vulnerable applications such as browsers, document readers, media files and runtime (ie. Flash, Java). Advanced mechanisms watch memory access routines to detect and block exploit techniques such as API caller verification, stack pivot, return-oriented-programming (ROP) and others. It must be equipped to tackle advanced, evasive exploits that targeted attacks rely on to penetrate an infrastructure.
	Able to have policy-based endpoint controls include the firewall, device control with USB scanning, thereby deterring and preventing installation of unrecognized applications, BYOD removable hardware devices such as USB flash drives, external hard drives and web content control with URL categorization.
	Capable of protecting through web security filtering that has real-time scanning of incoming web traffic, including SSL, http and https traffic, to prevent the download of malware to the endpoint. Anti-phishing protection automatically blocks phishing and fraudulent web pages.
	Able to provide protection against exploits in network vulnerabilities. It extends protected areas, now with network-based security that blocks threats like Brute Force attacks, Password Stealers, Network Exploits, lateral movements before they can execute.
	Able to protect email applications such as Outlook 2016, and SMTP/IMAP/POP3 clients through multilayered protection from known, unknown and emerging email security threats, mitigate large-scale phishing, targeted attacks.
	Capable of full disk encryption that uses Windows BitLocker and Mac FileVault, taking advantage of the technology built into the operating systems.

	Has a patch management feature which helps keep Operating Systems and Applications up to date across the entire Windows install base - workstations, physical servers and virtual servers
	Able to protect against Ransomware, even if malware or ransomware is modified, It must accurately detect new ransomware patterns, in both pre-execution and run-time mode.
	Able to leverage security intelligence in the cloud and takes advantage of its machine learning capability and event correlation to detect threats without noticeable impact on end users' tasks (low CPU and memory consumption).
	Able to instantly neutralize threats through actions including process terminations, quarantine, removal and rollback of malicious changes. It must be able to share threat information in real time to prevent similar attacks.
	Able to continuously compute a risk score to easily sort and prioritize assets, which makes it easy for the admin to address the most urgent issues.
	Must have an integrated and centralized management console that provides a single-pane-of-glass view for all security management components. It can be cloud-hosted or deployed locally, such as identifying Hostnames, IP and MAC Addresses, Operating System and patch updates, virus protection status, viruses detected and prevented. Must be capable of deploying remote installation on end-user devices. **ON-PREMISE CONSOLE OPTION** 1) Delivered as a virtual appliance and is available in the following formats: a. OVA (compatible with VMware vSphere, View) b. XVA (compatible with Citrix XenServer, XenDesktop, VDI-in-a-Box) c. VHD (compatible with Microsoft Hyper-V) d. Support for other formats and virtualization platforms may be provided on request. **CLOUD CONSOLE OPTION** security infrastructure hosted and maintained by the antivirus/endpoint security manufacturer: 1) Web console is instantly available online 2) Eliminate costs with servers and maintenance 3) Real-time control and monitoring of offsite and remote users with or without VPN
	Must be compatible and support the following operating systems: • Windows 10 (version 1909) or latest build, Windows Server 2019 or latest • Ubuntu 18.04 LTS or latest • Red Hat Enterprise Linux 8.x • MacOS

	Must also be compatible with mobile operating systems such as Android and iOS.
	Able to be compatible and support the minimum hardware requirements: 1) Minimum: 2.4 GHz single-core CPU Recommended: 1.86 GHz or faster Intel Xeon multi-core CPU 2) Memory: Minimum free RAM: 512 MB Recommended free RAM: 1 GB HDD space: 1.5 GB of free hard-disk space
Delivery date	Supply and delivery shall be made within thirty (30) working days from receipt of Notice to Proceed.

SERVICE LEVEL AGREEMENT	
Item	**Description**
Training	*INCLUSIVE of ONE (1) day installation and Administration Training (with Certificate), bundled with knowledge transfer and best-practice configuration and training for remote deployment and installation One (1) day extensive training (with Certificate), for up to five (5) attendees inclusive of lunch and product giveways
Technical Support	* Premium 8x5 Technical Support (1 Year) – with Dedicated Engineer Premium 8x5 Technical Support (unlimited Email and Phone Support) Mondays-Fridays, 8AM to 5PM with dedicated engineer *UNLIMITED 8x5 Standard Technical Support (unlimited Email, Chat and Phone Support) *UNLIMITED 24x7 International Support (Email, Chat, Phone & Remote Assistance) Premium twelve (12) 8x5 on-site visits within 12 months Max of 4 hours response time via phone or email and minimum of 24 hours for on-site visit
Updates	Security updates and software updates within maintenance period

IV. MODE OF PROCUREMENT

The mode of procurement shall be Small Value Procurement

V. NATURE OF PROCUREMENT

Classified as "Goods and Services", the antivirus or endpoint security subscription shall secure ICT assets and delivery of services in pursuit of all government undertaking by the Commission.

VI. SOURCE OF FUNDS AND APPROVED BUDGET FOR THE CONTRACT (ABC)

Source of Fund: Maintenance and other operating expenses, NPC 2020 Annual Procurement Plan, NPC ISSP (2019-2020)

The Approved Budget for the Contract (ABC) is Five hundred thousand pesos only (P500,000.00).

VII. INSTRUCTIONS TO BIDDERS

- The vendor must have PHILGEPS registration and must satisfy documentary requirements prescribed in the 2016 IRR of Republic Act No. 9184.
- Must accept 'send bill' payment terms.
- Must deliver the following and all technical and the SLA requirements abovementioned:
    a. Delivery, installation, configuration and technical support of endpoint security licenses/subscription with the NPC's Systems Administrator
    b. Software updates
    c. Warranty
    d. Technical support
    e. End users training

Republic of the Philippines
NATIONAL PRIVACY COMMISSION

VIII. EVALUATION PROCESS

Issuance of End User Acceptance Testing with attached screenshots or other related documents showing that the Anti-virus has been installed. It should be signed by the NPC Systems Administrator and IMISU Vice Chairperson and approved by the Head Executive Assistant.

IX. PAYMENT TERMS

Payment shall be made when the Service/Goods have been rendered or delivered in accordance with the signed contract and instructions set in the evaluation of service/goods delivered and upon issuance of Inspection and Acceptance Certification by the Inspection and Acceptance Committee.

Prepared by:

Sgd.
MOSLEMEN M. MACARAMBON JR.
Member
Interim Management Information System Unit

Reviewed by:

Sgd.
ROBELYN M. CRUZ
Vice Chairperson
Interim Management Information System Unit

Approved by:

Sgd.
VANDELFT R. IDANAN
Head executive assistant