NATIONAL PRIVACY COMMISSION

Republic of the Philippines
NATIONAL PRIVACY COMMISSION
BIDS AND AWARDS COMMITTEE

REQUEST FOR QUOTATION

ENDPOINT SECURITY SOLUTIONS (ANTIVIRUS)
(APP Item No. 2023-0008)

21 June 2023

NOTICE TO ALL PROVIDERS/SUPPLIERS:

The National Privacy Commission is intending to engage your service for the provision of **ENDPOINT SECURITY SOLUTIONS (ANTIVIRUS) (APP 2023-0008).** 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 **10:00 A.M., 29 June 2023.**

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

1. Copy of Valid and Current Mayor's/Business Permit issued by the city or municipality where the principal place of business of the prospective bidder is located;
2. PhilGEPS Registration Number;
3. Income Tax Return of the preceding year;
4. Notarized Omnibus Sworn Statement with applicable attachments[1]; and
5. 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:

BIDS AND AWARDS COMMITTEE
5th Floor, Ang Kiukok Hall,
PICC Delegation Building, PICC Complex,
Roxas Boulevard Manila 1307

Sincerely,

Digitally signed
by Medalla Joan
Therese Caragay

JOAN THERESE C. MEDALLA
BAC Secretariat Head
National Privacy Commission

[1] **NOTE:** Make sure to use the latest Omnibus Sworn Statement template downloadable from GPPB website (https://www.gppb.gov.ph/downloadables.php). Make sure that the "Jurat" of the sworn statement contains the details of the valid government issued ID of the affiant. Lastly, please make sure to submit its necessary attachments:
1. **If a sole proprietorship:** duly notarized Special Power of Attorney (if authorized representative)
2. **If a partnership, corporation, cooperative, or joint venture:** duly notarized Secretary's Certificate, Board/ Partnership Resolution, or Special Power of Attorney (whichever is applicable)

NOTE: Both the Omnibus Sworn Statement (OSS) and its attachment must specifically state the name of this procurement. Attached herein is the latest OSS template.

The original of this document is in digital format

TECHNICAL SPECIFICATION
ENDPOINT SECURITY SOLUTIONS (ANTIVIRUS)

ITEM	UNIT	QTY	Description/Specifications	Approved Budget of the Contract (Php 750,000.00)		Compliance (Manifest your compliance by <u>writing "COMPLY" in every item</u>)
				Unit Price	Total	
1	lot	1	- *Please refer to the "Technical Specification" for:* **A. Functional Description** 1. *General* 2. *Management Console*			
			B. Security Functions/Modules 1. *Anti-Malware* 2. *Intrusion Prevention and Prevention System* 3. *Firewall* 4. *Virtual Patching* 5. *Application Control* 6. *Event Tagging* 7. *Activity Monitoring*			
			C. XDR Platform Functions/Modules 1. *General Requirements* 2. *Correlated Detection Models* 3. *Triage and Threat Hunting* 4. *Threat Intelligence* 5. *Risk Analytics* 6. *Integrations and API Support* 7. *MITRE ATT&CK™ Mapping* 8. *Compliance & Certification* 9. *Endpoint Security Integration* 10. *Deployment services & maintenance*			
			D. Service Level Agreement			
			E. Supplier Qualification			
			F. Payment and Delivery *Within thirty (30) calendar days from receipt of Notice To Proceed (NTP)*			
			TOTAL			

Instruction to bidders (as applicable):

I. All prices shall be VAT inclusive.

II. Compliance must be stated by **<u>writing "COMPLY" in EVERY requirement</u>** mentioned above, failure to do so shall be a ground for disqualification.

III. Present the original Mayor's Permit and submit Certified True Copy of the eligibility documents and signed Quotation upon the scheduled signing of Notice of Award for inspection and verification.

IV. Acknowledgement of the Notice of Award shall be within five business (5) days from its issuance.

V. Delivery shall be completed within thirty (30) calendar days from receipt of Purchase Order/NTP.

VI. Delivery shall be made to NPC Office at 5F Delegation Building, PICC Complex, Vicente Sotto Avenue, Pasay City.

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

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

Republika ng Pilipinas

NATIONAL PRIVACY COMMISSION

Republic of the Philippines
NATIONAL PRIVACY COMMISSION

TECHNICAL SPECIFICATION

ENDPOINT SECURITY SOLUTIONS (Antivirus)
(APP Item No. 2023 – 0008)

I. Overview

The Interim Management Information System Unit (IMISU), which is acting as the management information technology division of the National Privacy Commission (NPC), is tasked with supporting, maintaining, and implementing layers of security in all information and communications technology (ICT) infrastructures of the National Privacy Commission. In this regard, the IMISU propose the subscription of an end-point security solution to secure and protect NPC endpoint devices like laptops, desktops, and servers. The solution will help to prevent the device or endpoint from being infected by malware (malicious software), uncover suspicious activity in the network, and to prevent cyberattacks.

II. Objective

To increase the security posture of the NPC and protect the security of all its issued endpoint devices from sophisticated attacks, an enterprise-level anti-virus and end-point security solutions must be properly configured, installed, and maintained on these endpoint devices.

With the current BYOD (bring your own device) and alternative work arrangements of NPC personnel, this current practice increases information security risk and threats; an antivirus and endpoint security solution is now a crucial requirement for the NPC to be secured. This is especially true for employees connecting to non-NPC networks using their workstations and laptops during fieldwork, telecommuting, and other alternative work arrangements. Hence, the need for endpoint security solutions that will monitor the behavior, identify, detect, prevent, and block these attacks, threats, malware, and ransomware is much needed.

III. Terms of Reference

A. Functional Description

1. General

a. The supplier must provide a minimum of 350 licenses for endpoint security with Extended Detection and Response (XDR) solution.

b. The solution uses a blend of advanced threat protection techniques to eliminate security gaps across any user activity and any endpoint that constantly learns, adapts, and automatically shares threat intelligence across environments.

c. The solution has the capability to automatically detect and respond to the ever-growing variety of threats, including fileless attacks and ransomware.

d. The solution must be able to provide insightful investigative capabilities, a rapid response for suspicious objects/activities and a centralized visibility across the network using an XDR platform.

e. The solution must support web reputation to prevent access to malicious web sites.

f. The solution combines machine learning with other advanced detection techniques for the broadest protection against multiple threats sources may it be known or unknown.

g. The solution must be able to clean infected files, perform rollback and even recover lost files if necessary.

h. The solution provides multiple integrated modules below providing a line of defense at the endpoint in single agent:

    i. Firewall
    ii. Intrusion Prevention (Desktop OS)
    iii. Anti-Malware + Web Reputation
    iv. Device Control
    v. Application Control
    vi. Endpoint Detection and Response (EDR) /XDR

2. Management Console

a. The solution must have a dashboard to display multiple information and must be **cloud managed.**

b. The solution must have a web-based management system for administrators to access using web browsers.

c. The management console must have "Alerts" on the main menu to view administrator notifications concerning system or security events.

d. The management console must have "System Events" to view a summary of security-related events, primarily for the Management server including Agents' system events. All administrative actions should be audited within the System Events.

B. Security Functions/Modules

1. Anti-Malware

a. The solution must be able to provide Web Reputation filtering to protect against malicious websites.

b. Must have Predictive Machine Learning to protect against unknown malware.

c. Must have Behavioral Analytics (against scripts, injection, ransomware, memory and browser attacks).

d. Must have Ransomware protection that has the ability to backup & restore encrypted documents.

e. Must have Pattern-based and signature-less high-fidelity machine learning for pre-execution and runtime.

f. Must have File Reputation - Variant Protection - Census Check - Web Reputation.

g. Must have Exploit Prevention (host firewall, exploit protection).

h. Must have Command and Control (C&C) protection.

i. Must have a combination of signature-based scanning and machine learning.

2. Intrusion Prevention and Prevention System

a. Must be able to provide Host Intrusion Prevention System (HIPS) / Host Intrusion Detection System (HIDS) feature agent.

b. Must be able to inspect deep packets that examine all incoming and outgoing traffic for protocol deviations, content that signals an attack, or policy violations.
c. Must be able to operate in detection or prevention mode to protect operating systems for desktop.
d. Must be able to provide protection against known and zero-day attacks.
e. Must have out-of-the-box vulnerability protection for over 100 applications, including database, Web, email, and File Transfer Protocol (FTP) services for server OS.
f. Must include smart rules to provide zero-day protection from unknown exploits that attack an unknown vulnerability, by detecting unusual protocol data containing malicious code.
g. Must have to exploit rules to stop known attacks and malware and are similar to traditional antivirus signatures in that they use signatures to identify and block individual, known exploits.
h. Must automatically shield newly discovered vulnerabilities within hours, pushing protection to large number of servers in minutes without a system reboot.

3. Firewall

a. Must include an enterprise-grade, bidirectional stateful firewall providing centralized management of firewall policy, including predefined templates.
b. Must have virtual machine (VM) isolation.
c. Must have fine-grained filtering (IP and MAC addresses, ports).
d. Must have coverage for all IP-based protocols (TCP, UDP, ICMP, GGP, IGMP, etc.) and all frame types (IP, ARP, etc.).
e. Must be able to prevent of denial of service (DoS) attacks.
f. Must be able to detect reconnaissance scans.

4. Virtual Patching

a. Provide virtual patching which shields vulnerable systems that are awaiting a security patch. Automatically shields vulnerable systems within hours and pushes out protection to thousands of VMs within minutes.
b. Must have vulnerability rules to shield known vulnerabilities from an unlimited number of exploits. Automatically shields newly discovered vulnerabilities within hours.
c. Must have the intelligence to provide recommended virtual patching rules to protect OS & Application.
d. Must be able to automatically unassign Virtual Patching rules after physical patch has been installed.

5. Application Control

a. Able to monitor changes made to the server compared to baseline software.
b. Able to allow or block the software and optionally lock down the server from unauthorized change.
c. Allows maintenance mode to allow installation of software and changes to the Operating System (OS).
d. Ability to manually input SHA-1 value to block specific files.

6. Event Tagging

a. The solution must support event tagging so that Administrator can add "tag" to events generated by the solution.

b. The Tag must be fully customizable; Administrator can add, edit and delete their own Tag with their own name.
c. The solution must be able to search for events based on the "Tag".
d. The solution must allow the administrator to specify a specific event that is to be automatically tagged by the system.

7. Activity Monitoring

a. The solution must be able to send security activity to a single data lake for central visibility of events across multiple vectors.
b. The solution must be able to provide effective expert analytics and global threat intelligence from the data collected in different modules.

C. XDR Platform Functions/Modules

1. General Requirements

a. The solution should provide more context with mapping to the MITRE ATT&CK TTPs for faster detection and higher fidelity alerts.
b. The solution should provide a platform for easier investigation with a graphical view and timeline of the attack.
c. The solution should have the capability to integrate with other 3rd party solutions via Application Programming Interface (API).
d. The solution must be capable to support incident response automation (Playbooks and customized response playbooks).

2. Correlated Detection Models

a. The Detection Models should combine multiple rules, and filters using techniques such as machine learning and data stacking. The detection model may use one or more filters to detect suspicious behaviors or events based on associated MITRE techniques.
b. The XDR console should provide the Administrator/Analyst detailed alert information in a unified view for more effective investigations, including a Summary and Highlights section, and Observable Graph section.
c. The XDR console should display the root cause analysis and provides additional information which might be beneficial to the investigation. The information should be displayed in a graphical way and as well presented in a table format.
d. The XDR console should display alerts triggered by Detection Models and allows the Administrator/Analyst to further investigate each alert.

3. Triage and Threat Hunting

a. The console should support the construction of powerful query strings to pinpoint the data or objects the Administrator/Analyst wants to examine.
b. After performing a search, the Administrator/Analyst should be able to export the search results as a CSV or JSON file.
c. Provides an attack-centric view of an entire chain of events across security layers. Easily run a root-cause analysis, look at the execution profile of an attack, and identify the scope of impact across assets.
d. The XDR console should assign a score to the alert and should calculate the score based on the severity of the matched detection model and the impact scope of the alert (such as the number of users, number of endpoints, servers, O365 email accounts, etc.).
e. Shall allow the analyst to actively hunt for threats within the infrastructure based on different hashes like MD5, SHA1 and SHA256, IP address, signer certificate, process

ID, original filename and filename on disk, whether has a Graphical User Interface (GUI).

4. Threat Intelligence

a. The solution should integrate up-to-the-minute intelligence reports from internal and external sources to help identify potential threats to your environment but not limited to the following:
   i. Internal Threat Intel.
   ii. Corporate security teams.
   iii. Government agencies from Europe and North America.
   iv. Information sharing organization.
   v. Security researchers.
   vi. Security vendors.

b. The XDR console should gather and integrate curated threat intelligence from internal and external sources.

c. The XDR console should allow the Administrator/Analyst to build custom intelligence by subscribing to 3rd party intelligence feeds using standards such as Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Intelligence Information (TAXII).

d. The solution should have access to the latest threat Indicators of Compromise (IOCs) like ransomware, Advanced Persistent Threats (APTs), malware, and the like.

5. Risk Analytics

a. The solution should have the capability to automatically assess, and correlate risk based on multiple factors - user identity, devices, network, data, apps, and infrastructure, before triggering an appropriate response based on the risk level.

b. The solution should have the capability to integrate with either or both cloud and on-premise identity access management (IAM) system for user authentication and access control.

c. The solution should have the capability to decrypt and inspect encrypted content over Hypertext Transfer Protocol Secure (HTTPS) connections to avoid virus/malware and other threats embedded in HTTPS traffic to pass unobstructed through security defenses.

d. The solution should be able to provide an overview of the company's risk exposure based on highly exploitable Common Vulnerabilities and Exposures (CVEs).

6. Integrations and API Support

a. The solution should have built-in integration with other well-established security providers for firewalls, vulnerability management, Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) vendors and when and should have API keys to allow third-party applications to access data through authorized accounts.

b. The solution should have the capability to allow integration with 3rd party solutions via API.

c. The XDR console should support APIs to automate common operations and procedures such as:
   i. Manage user accounts and roles.
   ii. Investigate and triage security events.
   iii. Perform responses during the investigation and advanced threat hunting.

7. **MITRE ATT&CK™ Mapping**
   a. The XDR console should list the events that are mapped into the MITRE ATT&CK framework, the Administrator/Analyst can use these events as starting point to do further investigations.
   b. The XDR console should detect events matching with behaviors mapped into the MITRE ATT&CK framework.
   c. The XDR console should list the events matching with the MITRE ATT&CK framework and should allow the Administrator/Analyst to filter the events based on criteria such as:
      i. MITRE Tactic ID.
      ii. MITRE Technique ID.
      iii. Risk Level.

8. **Compliance & Certification**
   a. Provides out of the box compliance support for:
      i. Payment Card Industry Data Security Standard (PCI DSS).
      ii. National Institute of Standards and Technology (NIST).
      iii. Health Insurance Portability and Accountability Act (HIPAA).

9. **Endpoint Security Integration**
   a. The solution must be able to integrate to SIEM.
   b. Directory integration so that it integrates with enterprise directories, including Microsoft Active Directory.
   c. Support selective module on agent installation.

10. **Deployment services & maintenance**
   a. The supplier shall provide the necessary test plans to ensure that all functional requirements are fully tested and sign off.
   b. The supplier shall ensure the personnel carrying out the deployment shall be certified professional by the vendor.
   c. The supplier shall provide preventive maintenance every 12 months to ensure all software patches and configurations are up to date and operating optimally.
   d. Training or equivalent for operational personnel administering the solution shall be included.
   e. Project Documentation shall be provided as follows:
      i. Submission of the project Implementation plan (including project schedule).
      ii. Submission of User Acceptance Tests & Results.
      iii. Submission of Administrator and User Guide.
      iv. Submission of Escalation Matrix and procedures.
      v. Extensive training for administrator and user.
      vi. Provide training certificates for up to five (5) attendees.

D. Service Level Agreement

1. Technical support must respond via telephone, mobile, or email to resolve technical and other related problems based on the Service Level Agreement (SLA), resolution must be delivered based on the following levels of severity. Additionally, the supplier shall submit an undertaking to have complied with Technical Specifications and Service Level Agreement Parameters below:

a. Severity Level 1, categorized as Critical, the issue must be resolved within 4 hours after the initial report to the service desk or customer support.
b. Severity Level 2, categorized as Major, the issue must be resolved at the soonest possible time (within 2 hours).
c. Severity Level 3, categorized as Minor, the issue must be resolved immediately (within 1 hour).

E. Supplier Qualification

1. PhilGEPS Registration
2. Mayor's/Business permit,
3. Notarized Omnibus Sworn Statement with applicable attachments (ABC above Php 50,000.00) and Income/Business Tax Return (ABC above Php 500,000.00)
4. Other documents as needed and prescribed under Revised IRR of Republic Act No. 9184.

IV. PAYMENT AND DELIVERY

Delivery shall be consistent with the following schedule of requirements:

Item	Quantity	Date of Delivery	Supporting Documents
End-Point Security Solution (Anti-virus).	1 lot	Within thirty (30) calendar days from the receipt by the Supplier of Notice to Proceed (NTP)/Notice of Award / Purchase Order (PO).	Instruction manual.

Place of Delivery: NPC, 5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307

Payment shall be made when the subscription has been delivered and in accordance with the Contract/Purchase Order and upon issuance of Certificate of Acceptance of Output (CAO) by the End User and Inspection Committee.

V. MODE AND NATURE OF PROCUREMENT

This shall be the procurement of Goods.
The mode of procurement shall be: ***Negotiated Procurement - Small Value Procurement (Sec. 53. 9)***

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

Source of Fund	:	Annual Procurement Plan FY 2023 (APP Item No. 2023 - 0008)
ISSP	:	NPC ISSP 2021-2023
Approved Budget for the Contract	:	Approved Budget for the Contract is Seven Hundred Fifty Thousand Philippine pesos only (Php 750,000.00).

Prepared by:

Digitally signed
by Plandor
Lennard Apora

LENNARD A. PLANDOR
Information Technology Officer II, IMISU

Recommending Approval by:

ATTY. RAINIER ANTHONY M. MILANES
Vice Chairman, IMISU

Approved by:

ATTY. IVIN RONALD D.M. ALZONA
Chairperson, IMISU
Executive Director

3.