TERMS OF REFERENCE

Procurement of Anti-Virus Paper License for FY 2024

I. Objectives

The main objective is to have protection, detection, and response with threat intelligence that will secure and protect DOT ICT infrastructures such as but not limited to servers, storage servers, databases, desktops, laptops, and other devices but also have a preventive measure against the newly developed virus, malware, ransomware, and other related issues.

II. Technical Specifications for Anti-Virus

Endpoint Security for Business for minimum 1000 Licenses.

Delivers a multi-layer anti-malware protection for smartphones, workstations and servers with end – point controls, mobile device management, encryption and systems management under a single, unified management console with additional feature of endpoint detection and response.

Features:

1. **Anti-malware (workstations and file server**)
   (a). The solution must have multiple anti-malware engines – with the combination of the traditional Signature-based, heuristic, Cloud-Assisted scanning and Machine Learning technology – for superior scanning and detection capability.
   (b). The solution should be able to provide security for heterogeneous IT environment. It shall support a range of platforms – including Mac, Linux and Windows – Including the new Windows 10 and Windows Server 2016 operating system.
   (c). Lightweight mode for Threat Protection ("Cloud mode"). Light antivirus databases with enabled KSN (require less RAM and drive space).
   (d). The solution should provide protection against new and unknown malwares. It should have an urgent detection system that may help protect the system against new threats, even before the release of a new malware signature.
   (e). The solution should be able to monitor the behaviour of applications automatically. It should have Behavioural Detection, Exploit, Anti-Rootkit and Remediation Engine that monitor the system – real time – and will detect any suspicious behaviour deeper within your system and application that rolls back actions done by malware.
   (f). The Solution should have Protection against encryption for shared folders unique anti-cryptor mechanism capable of blocking encryption of files on the shared resources from the malicious process running on another machine on the same network.
   (g). The solution should have a deeper level of protection that could work on the lowest level of a computers' operating system.
   (h). The Solution should have technologies that are improving its performance by estimating file threat level on the basis of its last modification date. File last

modification date is compared against its first scan date, creation date, and antivirus databases release date.

(i). The solution should have Host-based Intrusion Prevention System (HIPS) and personal firewall that would protect against hacker attacks. It should be able to control inbound and outbound traffic – by setting up parameters for an individual port, IP address or application.

(j). The solution should have a Network Threat Blocker mechanism that detects and monitors suspicious activity on your network. It should be pre-configurable on how the system should respond when suspicious behaviour is detected.

(k). The solutions should be able to auto-quarantine or auto-delete identified malwares without end-user interaction.

(l). The solution should be able to scan body text and attachments of incoming e-mail messages that are delivered through POP3 / IMAP mail clients.

(m). The solution should be able to block malicious/phishing URLs.

(n). The solution should be able to scan password protected compressed files for malicious programs.

(o). The solution should be able to re-launch itself automatically - when file server restarts - on events that the server experiences fault or suffering an unplanned shut down.

(p). The Solution should have AMSI Protection Provider. Antimalware Scan Interface (AMSI) allows a third-party application with AMSI support to send objects (for example, PowerShell scripts) to endpoint security solution for additional scan and to receive scan results for these objects.

(q). The Solution should be able to monitor and block abnormal behavior of applications.

(r). The solution should have the option of single agent for EDR and EPP (Endpoint Protection) that can be activated via licensing option.

2. End – point Controls

(a). Application Control

- The solution should be able to control application start up by blocking, granting or auditing each application upon launch.
- The solution should be able to monitor and classify each application as trusted, untrusted or restricted.
- The solution should be able to control whether an application is given access to specific system resources, such as the file system or the registry.
- The solution should be able to do Blacklisting and Whitelisting technology.
- The solution should have a dynamic whitelisting service that assesses the security of commonly used applications. Whitelist database should be updated regularly and automatically to ensure up-to-date protection.
- Policy should be able to use user account-based profile on the active directory.

(b). Device Control

- The solution should be able to allow administrator to set policy and control to any connected device, on any connection bus (not only USB), at any time.

- The solutions should be able to support device management and shall allow administrator to monitor, block or make the device Read-Only along with the option of providing exceptions.
- The solution should be able to block or allow devices based on specific serial number.
- The solution should be able to generate logs of events associated with deleting and saving files on USB device.
- The solution should be able to generate logs of list of trusted Wi-Fi networks, based on network name, encryption type, and authentication type.
- The solution should be able to monitor information about write and removal operations performed with files located on removable drives.
- The solution should have Anti-Bridging capability which blocks unauthorized commuting between networks.
- Policy should be able to use user account-based profile on the active directory.

(c). Web Control

- The solution should be able to filter each client's web browser usage. It should be able to permit, prohibit, limit or audit users' access to individual websites or categories of websites – including games websites, gambling sites or social networks.
- Policy should be able to use user account-based profile on the active directory.

3. Data Protection

(a). The solution should be capable of doing Full-Disk Encryption (FDE) and protects data on hard-drives
(b). The Solution should be capable of Bitlocker Management
(c). The solution should be able to do - pre-boot authentication – that is requiring users to pass through an authentication process before the operating system will even launch.
(d). The solution should be capable of doing single sign-on (SSO).
(e). The solution should be capable of doing File-Level Encryption (FLE).
(f). The solutions should be capable of encryption removable drive (USB) by means of Entire Drive Encryption and Portable Mode.
(g). The solutions should be capable of protecting data during transfer, storage and restoration, regardless of the policy settings at the endpoint to which the data is restored.
(h). The solution should be able to prevent exchange of encrypted files over IM or Skype, without restricting legitimate message exchange.
(i). The solution should be capable of providing mechanism for password recovery.
(j). Ability to recover disk data in case of hardware failures.
(k). The solution should be GDPR compliant.

4. Mobile Device Management and Security

(a). The solution should be able to configure and manage smartphones and tablets from a single console.

(b). The solution should be compatible with different mobile platforms – IOS and Android.
(c). The solution should be able to do – "Over the Air" Provisioning. It should be able to secure phones remotely by sending either an email or SMS containing a link to the corporate portal where users can download the profile and applications that administrator has approved.
(d). The solution should be able to detect rooted and jailbreak mobile devices to ensure compliance policy in the network.
(e). The solution should be able to enforce security settings such as camera disabling and force password.
(f). The solution should be able to control the applications that are being run in the mobile devices.
(g). The solution should be able to encrypt corporate data on mobile devices.
(h). The solution should have "Anti-Theft" mechanism for mobile devices.
(i). The solution should have multiple layer of anti-malware protection on mobile devices.
(j). The solution should have a 'CONTAINERIZATION" mechanism that will separate corporate data from personal data on mobile devices.

5. **System Management Tools**
(a). The solution should have operating system and application provisioning. Provide easy creation, storage, cloning and deployment of system images from a central location.
(b). The solution should be able to check operating system and other application vulnerabilities
(c). The solution should be able to patch Microsoft systems files and other 3rd party applications seamlessly. Patching should be automatic or scheduled.
(d). The solution should have license provision and control. It should have tools that could limit usage only to approved applications and versions - and restrict the number of licenses in use.
(e). The solution should have an asset inventory system that would list all hardware devices and software applications in the network. A notification should be sent to administrator once a new device has been found in the network.
(f). The solution should support "Wake-On LAN Technology" that would allow the solution to power-on workstations remotely during long hours of deployment or troubleshooting process.
(g). The solution should be able to assign workstations that would act as remote agent in a remote branch office for central update agent.
(h). The solution should have the capability to do remote and software installation from centralized management server.
(i). The solutions should have troubleshooting tools that can be use to remotely and securely connect to a client system to fix issues — from the same administration console.

6. **Unified Management Console**
(a). The solution should be capable of deploying applications such as end-point and third-party applications on a machine remotely.
(b). The solutions shall support Policy Enforcement
(c). The solutions shall provide dashboard with multiple information & these information should also be fetched from database based on different queries.

(d). The solution should be able to have automated mobile policies for devices that leave the corporate network.
(e). The solution should provide pre-defined policies as well as provide provision to change and customize policies based on groupings.
(f). The solution should have a single and unified management console to all its security and control features.
(g). The solutions should be able to manage mixed platforms in one management console.
(h). The solution should be able to support hierarchical grouping of machines and policy deployment. The grouping could be based on IP Address of a subnet of machines or a particular site.
(i). The solution should be able to provide a concise and accurate report that can be customize by the administrator.
(j). The solution shall support reporting in the following format like XML, HTML and or PDF
(k). The solution should have a web-interface that will be use to monitor the protection status and reports remotely.

7. Certification and Accreditations

(a). The solution should be recognized by ICSA Lab, NSS Lab.
(b). The solution must be certified by the following 3rd party testing organization: VB100, AV Comparatives – with +ADVANCE rating at least for 3 consecutive years.

8. Endpoint Detection and Response

(a). Architecture and Design

- The EDR solution must support integration with free of charge threat intelligence portal, which contains and displays information about the reputation of files and URLs.
- The EDR solution must support integration with cloud reputation service.
- The EDR solution must support central management and analytics through an on-prem Web console and cloud management console. (Incident-related data, System status and health check data, Settings, etc.)
- EDR agent must have integration with Endpoint Protection application.
- EDR and Endpoint Protection solutions must have unified console for administrators and analysts.
- EDR should support standalone agent installation (without Endpoint Protection application).
- Hardware platform where the solution is installed should be flexible for any upgrade include network interfaces, RAM and CPU

(b). Features

- Must provide an optimum Endpoint Detection and Response to stay safe in the face of complex and advanced threats by providing simplified investigation, advanced detection, and automated response, with simple root cause analysis.
- Capable to provides simple investigation tools, deep visibility, and automated response options in order to not just detect the threat, but to reveal its full scope and origins and instantly respond, preventing business disruption.

- Capable to perform and optimizing manpower resources and IT overheads by providing simple centralized controls and a high level of automation with a streamlined workflow from a single console available both on-premises and in cloud3.
- Compatible with existing AV

(c). Performance

- See security alerts on the endpoints and analyze them further to understand the full breadth and depth of the threat. This helps ensure the incidents are fully dealt with and no remainder of the threat is left on the endpoint.
- Must have enriches incidents with necessary information and helps the Agency understand connections between different events through attack spread path visualization.
- Set up automated responses for threats discovered across all endpoints based on IoC scans, or instantly respond to incidents upon discovery with 'single-click' options.
- Streamlined workflow from a single console available both on-prem and in cloud is coupled with simple EDR scenarios and controls, including drill-down visualization, IoC scanning and response options that don't require too much cybersecurity expertise or time.

(d). Detection

- The suggested solution must supplement verdict information from Endpoint Protection solution with system artefacts about the detection.
- The suggested solution must support auto generation of threat indicators (IoC) after detection occurs with ability to apply response action.
- The solution must have the capability to force run IoC scan across all endpoints with installed EDR agents.
- The suggested solution must support IoC scanning run according to a scheduler.
- The suggested solution must support import of third-party IoC in Open IoC format for its use in network scanning.
- The suggested solution must support scanning using auto-generated, uploaded or external (third-party) set of IoC's to detect earlier undetected threats.
- The suggested solution must support exporting of IoC generated by the solution to a file in OpenIoC format.
- The suggested solution must be able to perform the following actions:
  - Single Console
  - Threat Prevention
  - Data Protection
  - Hardening System
  - Response Action
  - Root cause analysis
  - Automation
  - IoC Scan
  - Sandbox features

(e). Visibility

- The suggested solution must generate detailed incident card related to the detected threat on an endpoint.
- An incident card must include at least the following information about detected threat: - Threat development chain graph (kill chain).
  - ❖ Information about the device on which the threat is detected (name, IP address, MAC address, user list, operating system).
  - ❖ General information about the detection, including detection mode.
  - ❖ Registry changes associated with the detection.
  - ❖ History of the file presence on the device.
  - ❖ Response actions performed by the application.
- Threat development chain (kill chain) graph must provide visual information about the objects involved in the incident, for example, about key processes on the device, network connections, libraries, registry, etc.
- An incident card must present detailed view on system artefacts and incident-related data for root cause analysis:
  - ❖ Process spawning
  - ❖ Network connections
  - ❖ Registry changes
  - ❖ Downloading object
  - ❖ Dropped objects, etc.

(f). Response

- The suggested solution must support 'Single-click" response form management console.
- The suggested solution must support at least the following response actions that an administrator can perform when threats are detected:
  - ❖ Prevent object execution:
    - ➢ EDR solution must support both modes: records to the events about attempts to launch objects or open documents that meet the criteria of the Execution prevention, but does not block launch or opening of these objects; blocks launch of the objects or opening the documents that meet criteria of the Execution prevention rules.
      - o EDR solution must support blocking objects by hash (MD5 or SHA256) or by path pattern.
      - o EDR solution must support blocking executables, scripts and documents
      - o EDR solution must support notification user about prevention option
  - ❖ Host isolation:
    - o EDR solution must provide means of isolating machine from the rest of the network in case of security incident, while preserving controlled.
    - o EDR solution must support creating custom host isolation rules (i.e. adding particular network resources to exclusion e.g. DNS or selecting predefined profiles).

- EDR solution must support manual bringing the host back online from isolation.
- ❖ Terminate a process on the device.
- ❖ Quarantine an object
  - The suggested solution must support object recovery from quarantine.
- ❖ Run system scan
- ❖ Remote program / process / command execution
- ❖ Start IoC scan for a group of hosts.

9. Administration and Reporting

(a). The solution must have a unified policies, centralized reporting and tasks execution within a Single-console for centralized management – on-prem or cloud based.

(b). Suggested solution management server must have ability to send logs to SIEM, SYSLOG servers.

(c). The solution must have different administrators functions that have a single interface/dashboard during sign on and controlled by privileges and rights based on their functions (Administrator, Reviewer, Investigator, etc.).

(d). The suggested solution must support secure communication between management console and endpoints with EDR agent.

(e). The suggested solution must support management of EDR agent through command line interface.

(f). Suggested solution must have inbuilt feature/module to collect the data required for troubleshooting, without require a physical access to the endpoint.

(g). EDR agent must have self-defense mechanism to prevent agent modifying agent-related files/system components entries etc.

(h). The solution must allow the creation of accounts with different roles used to administer the solution, just monitor the alerts, or review changes

(i). Administration server upgrade must not require installation from scratch and losing settings, etc.

(j). The solution should be able to send email notifications when certain types of security alerts are generated.

(k). The solution must support backup and restore the solution configuration.

(l). The solution should be simple to install and operate, and not require high-level skills from IT/Information Security staff.

(m). The solution should provide minimal impact on existing IT/Information Security staff load.

(n). The solution should be able to work in autonomous mode without access to external threat intelligence sources.

(o). Requirements for the solution documentation. A documentation for EDR software, including administration tools, should include at least online help for Administrators.

10. Additional Features

(a). The suggested solution must support integration with Sandbox with ability to automatically scan endpoints and apply responses in case if suspicious activity has been detected by the Sandbox.

(b). The suggested solution must support integration with APT solution.

(c). The suggested solution must support integration with Managed Detection and Response service.

(d). The suggested solution must support automated detection of malicious activity using Endpoint Protection solution and Sandbox.

11. Compliance, Maintenance and Support Level Agreement

(a). Have a reputable local vendor representative in the Philippines that has been active in providing cybersecurity protection/security and prevention for at least 7 years now.
(b). Supplier of the solution have at least two (2) certified engineers for end-point solution.
(c). Provides regular call or email check-up for concerns and product health monitoring even after sales.
(d). Available support through phone, email, web-remote assistance and on-site/on-call support.
(e). The local reseller as the first-level of support, the distributor as the second-level and the principal as the third-level of support.
(f). The supplier of the solution must be able to provide a comprehensive after-sales support and Maintenance agreement with options of 8x5, 8x7 SLA.
(g). 1 Day Product Training Certification for 8 pax.
(h). Free AV upgrade within the Warranty

12. Warranty

One (1) year subscription and services
With Quarterly onsite support and services

III. Budgetary Requirements

ITEM	TOTAL
Procurement of paper license for Anti-Virus	994,660.00

The total budget is Nine Hundred Ninety Four Thousand Six Hundred Sixty Pesos (Php 994,660.00) chargeable against OTDPRIM-ITD 2024 funds.

IV. Delivery

30 calendar days upon receipt of notice to proceed

V. Payment

Government Procedure

Project Officer:

Paul Brian D. Lao
OIC - Chief
ITD

Approved By:

Warner M. Andrada
OIC- Assistant Secretary, TD