COOPERATIVE DEVELOPMENT AUTHORITY

827 Aurora Blvd., Service Road, Brgy. Immaculate Conception Cubao, 1111 Quezon City, Philippines
http://www.cda.gov.ph helpdesk@cda.gov.ph CDA Philippines

BAGONG PILIPINAS

REQUEST FOR QUOTATION

Date: August 9, 2024
RFQ No.: 2024-176

Name of Company: _____
Address: _____
_____
Business Permit No.: _____
TIN: _____

Please quote your best offer for the item/s described below, subject to the Terms and Conditions provided at the dorsal portion of this request for quotation. Submit your quotation duly signed by you or your duly authorized representative not later than _____.

RAY R. ELEVAZO, CESE, MNSA
Chairman, Bids & Awards Committee

After having carefully read and accepted the Terms and Conditions, I/we submit our quotation/s for the item/s as follows:

ITEM DESCRIPTION	Quantity (QTY)	Approved Budget for the Contract	OFFER					REMARKS
			PRICE			Compliance with Technical Specifications (please check)		
PURPOSE: FOR THE OFFICIAL USE OF CDA HEAD OFFICE - ICTD		**₱755,000.00**	QTY	Unit Price	Total Price	Yes	No	
PROCUREMENT OF 1 YEAR OF SUBSCRIPTION OF FIREWALL WITH MONITORING AND 1 YEAR SUBSCRIPTION OF END-POINT SOLUTION	**1 LOT**							
TECHNICAL SPECIFICATIONS: **1. FIREWALL** 1.1 Inclusion of 1 Firewall License: Head Office (Renewal) 1.1.1 License ID Number: L0014781141 1.1.2 Base Firewall 1.1.2.1 General Management 1.1.2.2 Zone-based Firewall Features 1.1.2.3 Firewall, Networking and Routing 1.1.2.4 Base Traffic Shaping Quotas 1.1.2.5 Secure Wireless 1.1.2.6 Authentication 1.1.2.7 User Self Service Protocol 1.1.2.8 Base VPN Options 1.1.2.9 Single Ipsec and SSL VPN client Software 1.1.3 Network Protections Features 1.1.3.1 Intrusion Prevention (IPS) 1.1.3.2 Advanced Threat Protection and Security Heart Beat 1.1.3.3 Remote Ethernet Device (RED) VPN 1.1.3.4 Clientless VPN 1.1.4 Web Protection 1.1.4.1 Web Protection and Control 1.1.4.2 Cloud Application Visibility 1.1.4.3 Application Protection and Control 1.1.4.4 Web and App Traffic Shaping 1.1.4.5 Second Independent Malware Detection Engine for Dual-scanning 1.1.5 Sandstorm Protection Subscription 1.1.5.1 Sandstorm Cloud Sandbox Protection 1.1.5.2 Logging and Reporting *END-POINT SOLUTION / ANTIVIRUS Inclusion of 200 End-point/Antivirus Licenses License ID Number: D589395977 Integrated Management: - Must have a unified console for managing multiple products such as Advanced Endpoint Protection, Email Gateway, Server Security, Mobile Control etc. - All settings for these products MUST be configured from a Central Dashboard without the need to access additional consoles. Multi-Factor Authentication: - MFA must be enabled by default upon creation of central management account. - Must have the option to set MFA: All admins need MFA, Select admins who will need MFA, or No MFA needed. - Must have an option to have MFA using email, SMS, Google Authenticator, and native authenticator (by proposed solution) Multi-Platform Management:								

- Updating of endpoints should have the ability to set pre-configured available bandwidth used for both software updating and threat definition updates: 1) 64 Kb/s 2) 128 Kb/s 3) 256 Kb/s 4) 512 Kb/s 5) 1024 Kb/s 6) Unlimited								
- Must have the option to set up a local cache updating server within the on-premise network environment to minimize large software engine update. Relay must communicate all policy and reporting data to the central. - Must have the option to set up a relay on the same server as the local cache for devices that are not internet facing. - Must have an option for update management policy to customize the day and time when product updates become available to all or selected devices. Scheduled must not affect security updates, such as identities used to protect devices against new threats. Deployment Options: - Deploying the endpoint agent must support the following methodology: 1) Email setup link SIEM Integration: - Must have the capability to extract events and alerts information from the Cloud Dashboard to a local SIEM. API for Endpoint Management: - ust have APIs offered as RESTful HTTP endpoints over the public internet. - APIs must have the capability to query tenants, enumerate and manage endpoints and servers, and query alerts and manage them programmatically. **Role Management:** - Must provide admins the capability to assign predefined administrative roles to users who need access to the Admin Console. 1) Super Admin 2) Admin 3) Help Desk 4) Read-only - Access to management dashboard must support updated versions of: 1) Google Chrome. 2) Microsoft Edge. 3) Mozilla Firefox. 4) Apple Safari (Mac) Microsoft AD Synchronization: - Must have the capability to only allow outbound synchronization of Users/Groups from the local Active Directory servers to the Cloud Dashboard for policy management. Microsoft Azure AD Authentication: - Must have the capability to log in to the Admin Dashboard and Self Service Portal using Azure AD Login - Must have the capability to automatically login to the Admin Dashboard/Self Service Portal if already authenticated in the web browser with Azure AD login from a different application/service. Policies: - Selected policies should be able to be applied to either users or devices. - Policies must have the capability to be disabled automatically or expire based on a scheduled time and date. Enhanced Tamper Protection: - Must have the capability to prevent local administrative users or malicious processes from disabling the endpoint protection. - Must be able to export Tamper Protection passwords in CSV or PDF formats. - Must have the capability to prevent the following actions on the endpoint protection solution: 1) Stopping services from the Services UI 2) Kill services from the Task Manager UI 3) Change Service Configuration from the Services UI 4) Stop Services/edit service configuration from the command line 5) Uninstall 6) Reinstall 7) Kill processes from the Task Manager UI (desired) 8) Delete or modify protected files or folders 9) Delete or modify protected registry keys Threat Protection: - Must protect against multiple threats, both known and unknown, and provide a trusted and integrated approach to threat management at the endpoint.								

- Must protect endpoint systems against viruses, spyware, Trojans, rootkits, and worms on workstations and laptops regardless of their nature or the concealment mechanisms used.

- Must protect against threats related to executable files, as well as document files containing active elements such as macros or scripts. It must protect against exploits resulting from discovery (whether published or not) of security flaws in systems or software.

- Must have the capability to 'lookup' files in real-time to verify if they are malicious. This feature checks suspicious files against the latest malware in the vendor's Threat Intelligence database in the cloud.

- Must have the capability to detect low reputation files and have an action to prompt user or log only. Must be able to configure reputation level to either recommended or strict.

- Must have the capability to do real-time scanning of local files and network shares the moment the user tries to access them. The feature must include real time scanning for remote files. Access must be denied unless the file is healthy.

- Must have the capability to do real-time scanning of end-users Internet Access. It must monitor and classify the Internet websites according to their level of risk, and make this technology available to endpoint systems. A site known to host malicious code or phishing sites must be proactively blocked by the solution to prevent any risk of infection or attack against a flaw of the browser used. The solution must carry out checks against a database of compromised websites that are constantly being updated with new sites identified per day.

- Must protect managed systems from malicious websites in real-time, whether end-users work within the company or outside the company's secure network - at home or through public Wi-Fi. All browsers on the market must be supported (Internet Explorer, Firefox, Safari, Opera, Chrome, etc.)

Anti-rootkit Detection:

- Must identify a rootkit when reviewing an element without overloading the endpoint system. Rootkits must be proactively detected.

Suspicious Behavior Detection:

- Must be able to protect against unidentified viruses and suspicious

- Must have both pre-execution behavior analysis and runtime behavior

- Must be able to identify and block malicious programs before execution.

- Must be able to dynamically analyze the behavior of programs running on the system and detect then block activity that appears to be malicious. This may include changes to the registry that could allow a virus to run automatically when the computer is restarted.

- Must provide protection against buffer overflow attacks

Scanning:

- Must provide a scheduled scanner to run depending on the selected frequency or by manually triggering through Windows Explorer to scan the specified directories (local, remote or removable), with analysis parameters used, which may be different from the ones selected for real-time protection.

Advanced Deep Learning mechanism:

- The system shall be light speed scanning; within 20 milliseconds, the model shall able to extract millions of features from a file, conduct deep analysis, and determine if a file is benign or malicious. This entire process happens before the file executes.

- Must be able to prevent both known and never-seen-before malware, likewise must be able to block malware before it executes.

- Must protect the system even with offline and will not rely on signatures.

- Must classify files as malicious, potentially unwanted apps (PUA) or benign. Deep learning must also focus on Windows portable executables.

- Able to perform new Zero days threat scanning offline (without internet).

- Must be Smarter - should be able to process data through multiple analysis layers, each layer making the model considerably more powerful.

- Must be scalable - should be able to process significantly more input, can accurately predict threats while continuing to stay up-to-date.

- Must Lighter - model footprint shall be small, less than 20MB on the endpoint, with almost zero impact on performance.

- The deep learning model shall be trail and evaluate models end-to-end using advanced developed packages like Keras, Tensorflow, and Scikit-learn.

Exploit Prevention/Mitigation must detect and stop the following known exploits:

- Enforcement of Data Execution Protection (DEP)
Prevents abuse of buffer overflows

- Mandatory Address Space Layout Randomization (ASLR) Prevents predictable code locations

- Bottom-up ASLR Improved code location randomization

- **Null Page (Null Dereference Protection) Stops exploits that jump via page 0**
- Heap Spray Allocation Reserving or pre-allocating commonly used memory addresses, so they cannot be used to house payloads.
- Dynamic Heap Spray Stops attacks that spray suspicious sequences on the heap
- Stack Pivot Stops abuse of the stack pointer
- Stack Exec (MemProt) Stops attacker's code on the stack
- Stack-based ROP Mitigations (Caller) Stops standard Return-Oriented Programming attacks
- Branch-based ROP Mitigations (Hardware Augmented) Stops advanced Return-Oriented Programming attacks
- Structured Exception Handler Overwrite Protection (SEHOP) Stops abuse of the exception handler
- Import Address Table Access Filtering (IAF) (Hardware Augmented) Stops attackers that lookup API addresses in the IAT
- LoadLibrary API calls Prevents loading of libraries from UNC paths
- Reflective DLL Injection Prevents loading of a library from memory into a host process
- Shellcode monitoring Detecting the adversarial deployment of shellcode involves multiple techniques to address things like fragmented shellcode, encrypted payloads, and null free encoding
- VBScript God Mode Have the ability to detect the manipulating of the safe mode flag on VBScript in the web browser
- WoW64 Must have the ability to prohibit the program code from directly switching from 32-bit to 64-bit mode (e.g., using ROP) while still enabling the WoW64 layer to perform this transition.
- Syscall Stops attackers that attempt to bypass security hooks
- Hollow Process Protection Stops attacks that use legitimate processes to hide hostile code
- DLL Hijacking Gives priority to system libraries for downloaded applications
- Application Lockdown Will automatically terminate a protected application based on its behavior; for example, when an office application is leveraged to launch PowerShell, access the WMI, run a macro to install arbitrary code or manipulate critical system areas; the solution must block the malicious action – even when the attack doesn't spawn a child process.
- Java Lockdown Prevents attacks that abuse Java to launch Windows executables
- Squiblydoo AppLocker Bypass Prevents regsvr32 from running remote scripts and code
- CVE-2013-5331 & CVE-2014-4113 via Metasploit
In-memory payloads: Meterpreter & Mimikatz
- Dynamic Shellcode Protection Detects and blocks behavior of stagers
- EFS Guard Protection against Encrypting File System attacks
- CTF Guard Protects against a vulnerability in the "CTF" Windows component
- ApiSetGuard Prevents applications from side-loading a malicious DLL posing as an ApiSet Stub DLL

Advanced Exploit Mitigation:

- Must be able to protect against a range of exploits or "active adversary" threats such as the following:
1) Credential Theft Theft of passwords and hash information from memory, registry, or hard disk.
2) APC Violation Attacks using Application Procedure Calls (APC) to run malicious codes.
3) Privilege Escalation Attacks escalating a low-privilege process to higher privileges to access systems.
4) Code Cave Utilisation Malicious code that's been inserted into another, legitimate application.
5) Application Verifier Exploits Attacks that exploit the application verifier in order to run unauthorized software at startup.
- Must be able to mitigate exploits in vulnerable applications to protect the following:
a. Web Browsers
b. web browser plugins
c. Java applications
d. media applications
e. office applications

Malicious Traffic Detection (MTD):

- Must be able to detect communications between endpoint computers and command and control servers involved in a botnet or other malware attacks.

Intrusion Prevention System (IPS):

- Must be able to prevent malicious network traffic with packet inspection (IPS).

- Must be able to scan traffic at the lowest level and block threats before harming the operating system or applications. Anti-Ransomware Protection: - Must have the ability for the encrypted files to be rolled back to a pre-encrypted state. - Both Anti-Exploit and Ransomware protection does not need to have a Cloud Lookup to perform the detection. - Should a ransomware infection managed to get in, detailed historical tracking of where the infection originated and how it propagated will be reported courtesy of the Threat Cases (RCA). - Must be able to protect from ransomware that encrypts the master boot record and from attacks that wipe the hard disk. - Must be capable of local and remote detection. For instance, local detection is triggered when the ransomware is local to the server while remote detection is triggered when the ransomware is remote to the server, but attack files contained on the server, such as a share. AMSI Protection: - Must be able to protect against malicious code (for example, PowerShell scripts) using the Microsoft Antimalware Scan Interface (AMSI). - Must be able to scan code forwarded via AMSI before it runs, and the applications used to run the code are notified of threats. If a threat is detected, an event is logged.								
- Must have the ability to prevent the removal of AMSI registration on computers Data Loss Prevention (DLP): - DLP functionality must run on the same agent as the endpoint protection and all functions mentioned. - Must be able to monitor and restrict the transfer of files containing sensitive data. - Must have the capability to create custom DLP policies or policies from templates. - Must have DLP policy templates that cover standard data protection for different regions. - Must have the option to add custom DLP rule: 1) Content Rule 2) File Rule - DLP content rule must have the condition required for content scanning according to file content and destination. Actions must have options to either allow file transfer, allow transfer if user confirms, or block transfer. - DLP content rule must have the option to set exclusions based on file name and file type. - DLP content rule must have the option to set condition based on content control list (CCL). Must have the capability to add custom CCL and use filters by Region (e.g., Australia, Europe, India, Singapore, UK, USA, Global, Universal), filter by source (Custom, intelligence source (native to solution)), filter by type (e.g., Personally Identifiable Information (PII), HIPAA, PCI-DSS, Financial Data, Document classification, Health Care) - DLP file rule must have the condition required to check the destination of file and options for when file type matches and when file name matches. Actions must have options to either allow file transfer, allow transfer if user confirms, or block transfer. Must be able to scan different file types: Archive, Media container, Office password protected, Mail, Design, Plain text, Object code, Information rights management, Medical image formats, Image, Script/Markup, Document, Executable, Container, Spreadsheet, Encryption (native to proposed solution), Virtualization container, Disk container, Video, Audio, Database, Encryption, Presentation, Interactive media, and Science/Engineering. - DLP file rule must have the option to set the following destination: Email client, Internet browser, Instant messaging, Internet browser-external processes, Voice over IP, and Storage. Peripheral Control: - Must have the capability to control peripheral devices such as peripherals under the following categories: Bluetooth, Secure removable storage, Floppy drive, Infrared, Modem, Optical drive, Removable storage, Wireless, Media transfer protocol (MTP), and Picture Transfer Protocol (PTP). - Must have the capability to add device exemptions either by Model ID or Instance ID. - Must be able to set a customized desktop message to appear at the end of a standard notification in order to notify the user of policy violation.								

Application Control:

- Must have the capability to limit the applications needed for specific user groups.

- Must be able to detect and block application categories that may not be suitable for use in an enterprise environment. Must have an option for detetct controlled applications during scheduled and on-demand scans

- Must have out of the box application categories and built-in number of signatures per category to choose from such as Archive tool (9) Asset Management tool (14) Browser plug-in (39) Business intelligence tool (44) Digital imaging (31) Distributed computing (8) Document viewer (47) Download manager (62) Email/PIM client (30) ERP software (21) File sharing application (95) FTP client (15) Game (351) Instant messaging (138) Internet browser (96 Jailbreak software (3) Mapping application (6) Media conversion tool (15) Media player (142) Mobile Synchronization (37) Network monitoring/ Vulnerability tool (60) Office suite (48) Online storage (82) Proxy/VPN tool (120) System tool (215) Voice over IP (38)

- Must have a customized desktop messaging feature to the end of a standard notification to notify the user of policy violation

Web Control:

- Must be able to block risky downloads, protect against data loss, prevent users from accessing web sites that are inappropriate for work, and generate logs of blocked visited site.

- Must have security options to configure access to ads, uncategorized sites, or dangerous downloads.

- Must provide the administrator the ability to define "acceptable web usage" settings with built-in web categories (i.e., Productivity-related categories, Social Networking, Adult and potentially inappropriate categories, Categories likely to cause excessive bandwidth usage, Business-relevant site categories) in order to control the sites on which users are allowed to visit. Admin must have control access to websites that have been identified and classified in their own categories.

- Must have the option to Allow, Warn, and Block.

- Must have a data loss protection option that allows the administrator to control access to web-based email and file downloads, with choices of blocking the data, allowing data sharing, or customizing this choice.

Root Cause Analysis:

- Must have the capability to identify what happened, where a breach originated, what files were impacted, and provides guidance on how to strengthen an organization's security posture

- Must be able to record chain of events that occurred after an infection has been detected, enabling you to determine the origin of the infection, any resulting damage to assets, potentially exposed data, and the chain of events leading up to the halting of the infection.

- Shall provide a summary of the event via a graphical representation: What was the exploit discovered, where the beacon event occurred (an asset), when it occurred, how the infection succeeded.
- The graphical representation can be filtered to show full graph or direct path

- Shall provide recommendations to address the problem: Things to look for post-attack. Eg. Aside from files being restored from encrypted ones, check browser settings to ensure no vulnerabilities were created as a result of the infections.

- Activity Record allows administrators to add notes to the case. All case-related notes will be listed in this column.

- There are also buttons to enable the admin to modify the status of the case (New, In Progress, Closed) and to set priority (Low, Medium, High). When closing the threat case, the administrator can add notes to it.

- Shall provide a tabular view of everything affected during the attack. Items can be filtered based on type — e.g., files, processes, registry keys. The administrator can view information about each item, e.g., Filename (victim file or malware agent), process ID, start/stop timestamp of the event.

- Shall indicate the beginning of the root cause, charting out the series of events resulting from the attack as a collection of nodes. Each node contains specific information about files, processes, registry keys, etc. involved at that stage. The beacon event (marked with a blue dot) will be identified in the chain, but any events executed by the process identified as the beacon event will also be shown.

Advance System Clean:

- Must be able to cleanup threats detected by endpoint protection and exploit prevention. Must also be able to clean threats for PE files.

- Must be able to delet malware detected alerts from list when cleanup succeeds. - Must be able to clean ip PE (Portable Executable) files such as applications, libraries, and system files, even if automatic cleanup is turned off. Synchronized Security: - Must be able to work with other security products of the vendor to share information and respond to incidents. Endpoint + Email Gateway: - Must be able to automatically isolate compromised mailboxes, and clean up infected computers sending outbound spam and malware. Endpoint + Firewall: - Must be able to automatically isolate infected endpoints on the public and local area networks. - Must be able to identify all apps on the network. - Must be able to link threats to individual users and computers. Endpoint + Wireless Access Point: - Must be able to restrict internet access for infected endpoints connected to Wi-Fi automatically. Deliverables: - Provision of 1 Firewall License for the Head Office (Renewal) with License ID Number: L0014781141 for a 1-year period, to be delivered 30 days prior to the expiration date or on December 17, 2024. - Base Firewall Features - Network Protection Features - Web Protection Features - Sandstorm Protection Subscription - Logging and Reporting capabilities - Provision of 200 Endpoint/Antivirus Licenses with License ID Number: D589395977 - Integrated Management System - Multi-Factor Authentication setup - Multi-Platform Management capabilities - Configurable Updating Bandwidth Consumption - Deployment Options and SIEM Integration - API for Endpoint Management - Role Management and Microsoft AD Synchronization - Microsoft Azure AD Authentication setup - Policy Management and Enhanced Tamper Protection - Comprehensive Threat Protection and Anti-rootkit Detection								
- Suspicious Behavior Detection and Scanning capabilities - Advanced Deep Learning Mechanism - Exploit Prevention/Mitigation and Advanced Exploit Mitigation - Malicious Traffic Detection (MTD) and Intrusion Prevention System (IPS) - Anti-Ransomware Protection and AMSI Protection - Data Loss Prevention (DLP) and Peripheral Control - Application Control and Web Control - Root Cause Analysis and Advanced System Clean - Synchronized Security features - Other inclusions: - 24/7 Customer Support - Remote Deployment Services - Installation and Configuration for 20 nodes during business hours (9 AM to 5 PM) - One-day customized technical training. Budget and Funding: - The total budget allocated for this procurement is Seven Hundred Fifteen Thousand Pesos (PHP 755,000.00) Eligibility of the Contractor: - PhilGEPS registered. - In the IT business for at least 3 years.								

- Minimum 3 years of experience with government projects. Warranties of the Contractor: - The CONTRACTOR warrants strict conformity to the terms and conditions of this TOR. - The CONTRACTOR shall secure and maintain all necessary registrations, licenses, and permits. - No assignment, transfer, pledge, or sub-contracting of any part or interest is allowed. Delivery Period: - The service provider must deliver all the required services within 30 days prior to expiration date or on December 17, 2024, upon receipt of the Notice to Proceed (NTP). Terms of Payment: - Payment will be made according to the following schedule: - 100% of the contract amount upon signing of the contract, issuance of the Notice of Award, Notice to Proceed, and upon successful delivery, conduct of training and acceptance of all deliverables listed above. - Payment will be made upon provision of licenses, subject to required Final Withholding VAT (5%) and Expanded Withholding Tax (2%). - Payment shall be processed within a reasonable time upon submission of documentary requirements, including Sales Invoice/Billings and Certificate of Acceptance issued by CDA ICTD. - No advance payment will be made as per Section 88 of PD 1445. Confidentiality: - The service provider shall maintain the confidentiality of all data and information related to the Cooperative Development Authority (CDA) and its operations. Pre-Termination of Contract: - The CONTRACTOR shall be liable for additional liquidated damages equivalent to 1% of the contract price in case of pre-termination. - The DBM reserves the right to blacklist the CONTRACTOR in case of pre-termination. Contact Information: MR. RONALDO G. RIVERA Information Technology Officer II Information and Communications Technology Division (ICTD) Cooperative Development Authority									

Note: •Quoted price/s must be VAT inclusive.
•Supplier must have a Land Bank of the Phil. Account.
•Supplier must submit a sealed quotation.
•Sealed quotation must be submitted together with the following requirements: Company Profile, DTI/SEC Registration, Business/Mayor's Permit, BIR Registration, and PhilGEPS Certificate of Membership

Signature over Printed Name

Canvasser

Contact Numbers (Landline and/or Cellphone Nos.)/E-mail address