Republic of the Philippines
Department of Justice
PAROLE AND PROBATION ADMINISTRATION
DOJ Agencies Bldg., NIA Road corner East Avenue,
Diliman, Quezon City 1101
Telefax (02) 927-6821 or Email: dojppapropertysection@gmail.com

BAGONG PILIPINAS

RFQ No. 2024 - 083

REQUEST FOR QUOTATION

Line Item No.	Description	Procure-ment Mode	Quan-tity	Unit	Unit Price	TOTAL
1	**Supply, Delivery, and Installation of the ICT Software Subscription Requirements for the Endpoint Anti-Virus for the Enhancement and Maintenance of Information Systems** *(see attached Terms of Reference)*	SVP	1	Lot		
Purpose: For the renewal of the Anti-Virus Licenses.						

Requested by:

SAO MARISSA M. ABERION
OIC, Administrative Division

Canvassed by:

SIR R. BIRION
Buyer/Canvasser

DEALER'S INFORMATION

Supplier's Profile	Terms and Conditions
Business Name: _____ Business Address: _____ Contact Number/s: _____ _____ _____ (Signature Over Printed Name of Authorized Representative) (Date Signed)	1. Payment Terms: [ ] w/in 30 C.D. upon delivery [ ] Cheque-On-Delivery 2. Delivery Terms: [ ] FOB Destination (Delivery) [ ] FOB Destination (Pick-up) 3. BIR Registration: [ ] VAT [ ] Non-VAT 4. TIN: _____

Republic of the Philippines
Department of Justice
PAROLE AND PROBATION ADMINISTRATION
OFFICE OF THE ADMINISTRATOR
DOJ Agencies Building, NIA Road, Quezon City
Tel. No. (02) 8925-0235 / (02) 8929-3145
email: aodojppa@gmail.com

BAGONG PILIPINAS

TERMS OF REFERENCE
SUPPLY, DELIVERY AND INSTALLATION OF ICT SOFTWARE SUBSCRIPTION FOR THE ENDPOINT ANTI-VIRUS FOR THE ENHANCEMENT AND MAINTENANCE OF INFORMATION SYSTEMS

DELIVERABLES:

Lot	Quantity	Description	Approved Budget for the Contract (Php)	Delivery Period
1	152	ICT Software Subscription (Renewal of Endpoint Anti-Virus Requirements)	612,256.00	Within sixty (60) calendar days from date indicated in the Notice to Proceed
Total Amount			**612,256.00**	

TECHNICAL SPECIFICATIONS:

PARTICULARS	SPECIFICATIONS
Endpoint Antivirus – Branded and complies with the following minimum requirements:	
Endpoint Antivirus Security	**Centralized Management and Graphical Reporting**
	Should be capable of being managed via a centralized console, should be capable of deploying antivirus on all desktops and laptops attached to the network centrally and should provide reports such a AV Coverage, Virus Definition update reports, actions performed etc.
	Should provide a mechanism for developing and deploying policy to each system node with respect to scheduling scan jobs, real-time scan settings, signature distribution, alerting and analysis etc.
	Should allow the Administrator to initiate virus sweeps remotely in case of an outbreak.
	Should be capable of deploying, updating, configuring and monitoring all the users with centralized administration of all Endpoint Protection components on simple and complex networks.

PARTICULARS	SPECIFICATIONS
Endpoint Antivirus (cont.)	
	Should have a single and configurable installation with centralized configuration, and policy management should have a common distribution mechanism via combination of push and pull technology for better management
	Should be capable of pushing client installation and update anti-virus software, virus definitions and policies automatically to clients and servers from a centralized location and it should also support manual installation of client via network share
	Should have automatic update of antivirus server from vendor site, and client should get update from the local server and if updating from the primary server fails for any reason (such as the user being off the network) an attempt should be made to contact the secondary server (i.e vendor site)
	Active Directory Support
	Should support integration with active directory for directory structure of computers for better management and should have logical group based on IP addresses (Subnets)
	Should support scanning of Active Directory Database and also must scan compressed file formats like ZIP, RAR, TAR, etc.

PARTICULARS	SPECIFICATIONS
Endpoint Antivirus (cont.)	
	Scans and Antivirus
	Should automatically scan external devices (floppy disks, compact disks, USB devices, and network shares in real-time when accessed) as soon as they are attached to PC, server, laptop etc.
	Should allow the user/administrator to initiate a scan on the memory as well as the HDD
	Should have the ability to exclude specific files and directories from the On Demand Scanning
	Should allow the user to scan files which supports reputation based scanning or any other methods similar to this facility like user defines processes/files as high risk or low risk and thereby assign a scan policy on them
	Should allow the user/administrator to run at specific times or at scheduled intervals and update at the endpoints from central server
	Should provide Web antivirus features which should analyze site address and block access to dangerous sites and scan the object downloaded over HTTP
	Should have the ability to include on demand or scheduled in-memory process scanning for viruses, worms and Trojans. Memory Scanning should use viral signatures instead of file names
	Should protect from the threats that e-mail message may contain and messages should be intercepted at the protocol level and by embedding into the most popular mail clients

PARTICULARS	SPECIFICATIONS
Endpoint Antivirus (cont.)	
	Should provide scanning capabilities for POP3, and IMAP mail traffic, protecting email communications from one of the most common channels of malware attack
	Should enable smart optimization or any similar functions such as allowing the On Demand Scanner to recognize the last scanned file and resume scanning from that file if an "On Demand Scan" is interrupted
	Should provide instant messaging antivirus features which should protect from the threats that instant messaging attachment may contain and it should support instant messaging applications: e.g., ICQ, MSN, AIM, MAIL, RU AGENT and IRC
	Spyware, Adware and Dialer Detection
	Should be capable of detecting, discovering, discerning and removing unwanted programs in real time malicious software including viruses, spyware, malware, trojan horses, worms, adware, dialers, grayware, madware, joke programs, remote administration tools, password crackers, keylogger, user defined programs, rootkit and ransom ware.
	Should have anti malware for network storage
	Post detection action
	Should perform the following post detection antiviral actions: Alert / Notify, Clean, Delete / Remove, Move / Quarantine, Prompt for Action
	Should allow the Administrator to have the option of excluding specific programs that are detected as part of this detection. The exclusion can be set based on filenames or categories

PARTICULARS	SPECIFICATIONS
Endpoint Antivirus (cont.)	
	Should provide a feature for detection, cleaning, quarantine, deleting malware/viruses
	Protection
	Should have the capability to clean, quarantine, delete viruses and detect new classes of viruses by normal virus update mechanisms
	Should have the capacity to prevent infections from occurring by detecting and preventing the execution of malicious code that leverages, Java Scripts, Visual Basic (VB) Scripts
	Should provide a web console feature that works via a browser. The web console should be used for creating reports and performing simple operations with computers i.e., viewing the status, relocating, installing Antivirus
	Should provide Application Privilege Control to regulate the activities of the running programs, namely, access to the file system and registry as well as interaction with other programs
	Should provide web filtering enforced on the endpoint whether users are on or off the corporate network
	Should provide protection which include anti-virus, anti-malware, Host-Based Intrusion Prevention System (HIPS) and malicious traffic detection

PARTICULARS	SPECIFICATIONS
Endpoint Antivirus (cont.)	
	Should have HIPS module which could protect the endpoint from network based attacks. The signatures for HIPS should be regularly updated to identify latest network attacks for endpoints.
	Should have a feature to detect network attacks originating from a computer, and then block the traffic from that computer
	Should provide device-control module with ability to control usage of unknown or unwanted devices, reducing the risk of data loss, White list categories (based on serial numbers), Temporary grant access to block device over the internet, and device inventory.
	Should provide Web control feature with URL filtering and categorization together with web action that can allow, block, kick, delete, and warm users with viruses.
	Should provide tamper protection features i.e., user who does not know the password may not able to change the existing policy, exit or uninstall the antivirus solution
	Should provide malicious traffic detection

PARTICULARS	SPECIFICATIONS
Endpoint Antivirus (cont.)	
	Should have predefined rules for hundreds of the most commonly used applications to reduce time spent on configuring the firewall
	Should passed on to administrator the alerts on virus activity
	Should have small protection updates – typically under 10-50 in file size
	Supported Platforms
	Should support multi - platform operating system(Windows , Mac, Linux) and the same should be managed from a single centralized management console
	Should have browser compatibility: latest Microsoft Internet Explorer / Mozilla Firefox / Apple Safari / Google Chrome, etc.
	Subscription
	Endpoint Anti-virus Enterprise with 3 years subscriptions
	Vendor
	Vendor is a manufacturer-authorized reseller of the anti-virus
	Services
	Installed and configured to the desktops and laptops before deployment to other offices
	Live web chat, email, online help or onsite visit if necessary
	The Bidder is required to integrate the anti-virus to the existing management console
	Licenses and subscriptions are expected to start upon installation
	Provide unlimited support knowledge base access
	Provide software downloads, updates and maintenance
	Provide access to support forums