PhilGEPS Philippine Government Electronic Procurement System — Central Portal for Philippine Government Procurement Oppurtunities

Help

# Bid Notice Abstract

## Request for Quotation (RFQ)

| | |
|---|---|
| **Reference Number** | 5771413 |
| **Procuring Entity** | BUREAU OF THE TREASURY |
| **Title** | PROVISION OF ANTIVIRUS SOFTWARE FOR VARIOUS SERVER ASSETS OF THE BUREAU OF THE TREASURY |
| **Area of Delivery** | Metro Manila |

| | |
|---|---|
| **Solicitation Number:** | 2018-10-0474 SAD |
| **Trade Agreement:** | Implementing Rules and Regulations |
| **Procurement Mode:** | Negotiated Procurement - Small Value Procurement (Sec. 53.9) |
| **Classification:** | Goods |
| **Category:** | Information Technology Parts & Accessories & Perip |
| **Approved Budget for the Contract:** | PHP 970,000.00 |
| **Delivery Period:** | 60 Day/s |
| **Client Agency:** | |
| **Contact Person:** | Mr. Clarence Bolante Bunan<br>Administrative Officer III<br>Ayuntamiento Building, Cabildo St., cor. A. Sorian<br>Intramuros, Manila<br>Manila<br>Metro Manila<br>Philippines 1002<br>63-2-6632206<br>63-2-5247008<br>cbbunan@treasury.gov.ph |

| | |
|---|---|
| **Status** | **Pending** |
| **Associated Components** | 1 |
| **Bid Supplements** | 0 |
| **Document Request List** | 0 |
| **Date Published** | 06/11/2018 |
| **Last Updated / Time** | 05/11/2018 09:59 AM |
| **Closing Date / Time** | 09/11/2018 12:00 PM |

**Description**

PROVISION OF ANTIVIRUS SOFTWARE FOR VARIOUS SERVER ASSETS OF THE BUREAU OF THE TREASURY

Brief Description:
This project calls for the provision of Antivirus software licenses and support for the protection of various Server assets of the Bureau. The acquisition and installation of server antivirus is aimed at providing additional protection to the Bureau's Server assets against various forms of virus and malware attacks from internal and external sources.

TECHNICAL SPECIFICATIONS:
1. Server Antivirus Licenses
1.1. Quantity: 70 Licenses

2. Server Antivirus General Features
2.1. Enterprise Console
2.1.1. A single, automated console for Windows, Mac, Linux and virtualized platforms centrally deploys and manages antivirus and client firewall protection; intrusion prevention; endpoint web protection; patch assessment; encryption; data, device and application control; and endpoint assessment and control.
2.2. System Protection
2.2.1. Component of the endpoint protection software providing coordination between detection engines and

performing lookups as required ensuring the most up to date protection.
2.3. Enhanced Runtime Behavior Detection
2.3.1. Should detect writing to the registry, calling a Windows API; looks at pre-execution analysis results - source of files, packers used, other suspicious rule trigger.
2.4. Browser Exploit Prevention
2.4.1 Man-in-the-Browser Detection, reveals intruders that manipulate critical browser functions. Prevent attackers from hijacking control flow of internet facing applications, like web browsers.
2.5. Patch Assessment
2.5.1. Scans and identifies computers missing critical patches for vulnerabilities commonly targeted by threats.
2.6. Anti-virus for Virtual Environments
2.6.1. Protects virtual environment, whether it is running on VMare vSphere on Microsoft Hyper-V. Provides efficient, always-on security for guest machines by offloading malware detection to centralized Security Virtual Machines. Real-time threat protection for virtual machines with automatic clean up, centralized scanning with low resource usage. Simplified manage console to view alerts, scans, create policies and generate reports.
2.7. Central Management
2.7.1. Platform Supported
2.7.1.1. Windows SBS 201/ Windows Server 2003 and R2/ Windows Server 2008 and R2/ Windows Server 2012 and R2/ Windows Server 2016.
2.7.1.2. Supported Linux Distributions (On Premises)
2.7.1.2.1. Amazon Linux
2.7.1.2.2. CentOS 6/7
2.7.1.2.3. Debian 8/9
2.7.1.2.4. Novel Open Enterprise Server 2015 SP1
2.7.1.2.5. Oracle Linux 6/7
2.7.1.2.6. Red Hat Enterprise 6/7
2.7.1.2.7. Red Hat Enterprise Linux 6 32-bit version supported until Nov 30th 2020
2.7.1.2.8. SUSE 11/12
2.7.1.2.9. Ubuntu 14/16/18"
2.7.2. Database Platforms Supported
2.7.2.1. SQL 2005, 2008 Express Edition/SQL 2012, 2014, 2016 Express Edition/SQL 2008, 2012, 2014, 2016
2.7.3. Central Deployment , Configuration and Reporting
2.7.3.1. Ability to discover, deploy, update configure and monitor clients with centralized administration of all server protection components on simple and complex networks.
2.7.3.2. Endpoint discovery (with and without agent; active and inactive devices) - Active Directory synchronization, network discover an IP range.
2.7.3.3. Deployment options:
2.7.3.3.1. Protect computer wizard
2.7.3.3.2. Active Directory synchronization
2.7.3.3.3. Push deployment via script
2.7.3.3.4. Manual (Locate installers for protecting computers manually)
2.7.3.4. Microsoft Active Directory synchronization
2.7.3.4.1. Automatic computer discovery and synchronization with AD structure
2.7.3.4.2. Automatic installation of newly discovered endpoint.
2.7.3.5. All settings for server protection will be configured from central management console without the need to access additional consoles.
2.7.3.6. Must have integrated reporting that delivers instant and scheduled report of the threat alerts, infections and at-a-glance report for outbreak risk. Support report output in PDF, HTML, Excel, Word, RTF, CSV, XML.
2.7.3.7. Actionable security dashboard can perform full scan, cleanup and remediation.
2.7.3.8. Monitors applications launched on the endpoints, removable devices and data that are forwarded or transmitted.
2.7.3.9. Monitor and control suspicious behavior like registry or critical windows system files modification.
2.7.3.10. Rootkit detection and cleanup
2.7.3.11. Detects, block and clean up known and unknown threats, included virus, spyware, adwares and PIAs.
2.7.3.12. Antivirus with Intercheck technology.
2.7.3.13. Intercepts and scans files as they are accessed.
2.7.3.14. Assess computers for missing patches.
2.8. Policy-based Administration
2.8.1. Must have policy-based management; centralized policy covering updating schedules, antivirus and HIPS, client firewall, application, device and data control.
2.8.2. Centralized policy covering updating schedules, Antivirus and HIPS, client firewall, application, device and data control.
2.8.3. Can create subgroups (sub-estates) to create an entire tree, all subgroups inherit the policies applied to the parent group.
2.9. Role-based Administration
2.9.1. Have the capability to allow the separation of estate management to different administrator login.
2.9.2. Delegate part of the administration to a list of administrators with restricted permissions.
2.9.3. Can create custom roles that will suit to needs and can be are assigned to Windows users or Windows groups.
2.10. Tamper Protection
2.10.1 Prevents users from uninstalling the antivirus, auto update, client firewall, remote management system and disk encryption on a windows computer.
2.10.2. Policy is configured within Enterprise Console.
2.10.3. Requires password to be set for protection and can only be configured on the endpoint if the user has administration rights or the correct password is entered.
2.11. Dashboard and Reporting.
2.11.1. Integrated graphical reporting delivers instant and scheduled email report of the threat alerts and infections

while the security dashboard gives an at-a-glance report for outbreak risk.
2.11.2. Near real-time view of the security health of the organization through the use of dashboards or similar technology.
2.11.3. Automated email reporting when certain alert threshold is reached.
2.11.4. Support report output in PDF, HTML, Excel, Word, RTF, CSV, XML.
2.12. Signature Updates
2.12.1. Small updates size with an average of 50KB per signature update.
2.12.2. Ability to check for updates as often as every 10 minutes.
2.12.3. Separate schedule for signature and software updates.

3. Server Protection
3.1. Server platform Supported
3.1.1. Win SBS 2011/ Server 2008 including COre/R2 including Core, Server 2012 including Core/2012 R2 including Core, Server 2016/.
3.2. Virtualization Platforms Supported
3.2.1. "VMware vSphere/ESX 2GB 2Gb 2
3.2.2. VMware Worktation
3.2.3. Microsoft Hyper-V Server
3.2.4. Citrix XenServer"
3.3. Hot Instruction Prevention System
3.3.1. Guarding against unknown threats by analyzing behavior before code executes.
3.3.2. Integrated with endpoint protection agent.
3.3.3. Stop zero-day threats with built-in HIPS Behavioral Protection.
3.3.4. Suspicious Behavior Detection
3.3.5. Buffer Overflow Protection.
3.4. Runtime Protection
3.4.1. Monitor and block suspicious behavior like registry or critical windows system fiels modification.
3.4.2. Protection against buffer overflow.
3.5. Application Control
3.5.1. Selectively authorize or block legitimate Applications that impact network bandwidth, Systems availability, and user productivity.
3.5.2. Integrated with endpoint protection agent.
3.5.3. Monitor applications launched on the endpoints. removable devices and data that are forwarded or transmitted.
3.5.4. Vendor-managed list to offload the administrator from monitoring new applications or specific categories of applications.
3.5.5. Provides and automatically updates the list of controlled applications.
3.5.6. Integrated in unified detection engine.
3.5.7. Policy set in central management console.
3.5.8. Allows different policies for different groups.
3.5.9. Can enforce company policies as well as reduce security risks.
3.5.10. Stop instant messaging, games, peer-to-peer applications who consume bandwidth.
3.5.11. Prevent confidential information from being exposed via peer-to-peer exchange or transmitted via instant messaging.
3.6. Device Control
3.6.1. Control the use of removable storage, optical media drives and wireless networking devices and define which computers have access to specific removable devices.
3.6.2. Integrated with endpoint protection agent.
3.6.3. Should be port-agnostic and should support whatever port is used to connect the device like USB, FireWire, SATA, and PCMCIA interfaces.
3.6.4. Able to control the use of MEdia Transfer Protocol (MTP) and Picture Transfer Protocol (PTP) devices, removable storage, optical media drives and wireless networking devices.
3.6.5. Ability to set storage devices in "Ready-only mode" to prevent data from being written.
3.6.6. Must prevent wireless bridging (ex. Disables wireless when Ethernet is connected protecting our netwrok from backdoor connections).
3.6.7. Supports device instance and model exceptions.
3.6.8. Easy authorization of allowed devices.
3.6.9. Integrated in unified detection engine.
3.6.10. Policy set in central management console.
3.6.11. Allows different policies for different groups.
3.6.12. Block windows from bridging two networks.
3.7. Web Protection
3.7.1. Block URLs that are hosting malware.
3.7.2. Live in-the-cloud lookups check database of Millions of compromised sites.
3.7.3. Protects users everywhere, in the office, and when not behind corporate protection, i.e. at home or over public WIFI.
3.7.4. Integrated into existing endpoint agent with no endpoint configuration required.
3.7.5. Online scanning for malware (in the cloud).
3.7.6. Runtime HIPS/behavior combination.
3.7.7. Ability to detect and block compromised / hijacked trusted sites.
3.7.8. Multi-web browser support.
3.7.9. Provides control of the Internet regardless of the browser used through "Web LENS" technology (Web Lightweight Endpoint Scanner).
3.8. Web Control
3.8.1. Control access inappropriate website.

3.8.2. Create Web control policy from enterprise console and apply to the right PC group.
3.8.3. Add own list of URLs or IP address via exceptions tab.
3.9. Data Loss Prevention
3.9.1. The End Point must come with Integrated with data loss prevention where it enables you to monitor for the transfer of sensitive data, such as Personally Indentifiable Information (PII) or company confidential documents. Data Loss Prevention should reduce the risk of this data being accidentally saved to removable storage device or sent out of the organization.
3.9.2. Data Loss Prevention must be able to stop users from transmitting sensitive documents from the following medium:
3.9.2.1. Removable storage
3.9.2.2. Optical and disk drives (CD/DVD/BD/Floppy)
3.9.2.3. Internet enabled applications (web browser, email client, instant messenger client)
3.9.3. Must be able to set a File Matching rule to various source like Email Clients, Internet Browser and Storage Devices.
3.9.4. Must have predefined File-Type Groups provided by the vendor.
3.9.5. Must be able to detect File Matching rules based on:
3.9.5.1. True File Type
3.9.5.2. File Name
3.9.6. Must be able to set a Content Matching Rule to various source like Email Clients, Internet browser and Storage Devices.
3.9.7. Must have pre-defined Content Control List (CCL) from vendor containing rules to detect Personally Identifiable Information (PII), Financial details, Confidential Markers which is constantly updated by the vendor.
3.9.8. Must be able to define custom Content Matching rule with support for strings detection and regular expression rules for more complex detection.
3.9.9. Must have the ability to enforce content matching Data Loss Prevention rules based on:
3.9.9.1. Predefined content rules from principle (e.g. credit card numbers, social security numbers, postal addresses, or email addresses)
3.9.9.2. Custom Content Rule

4. Other Requirements
4.1. Product must be in the Garther Leaders Magic Quadrant in endpoint protection for the year 2018.
4.2. License and support coverage: 3 years

5. Training and Technical Support
5.1. Installation and configuration of the management software.
5.2. Installation and/or .dat file update for central office target installations.
5.3. 24x7 phone, email, live chat and remote support.
5.4. 8x5 onsite support, if necessary
5.5. Quarterly visit and systems maintenance check-up.
5.6. Training on the installation, deployment, administration and management of the antivirus software, to be scheduled within 60 days from date of acceptance.

6. Delivery Period
6.1. 60 days from the date of receipt of Purchase Order

7. Mode of Payment
7.1. Lump Sum. Upon delivery of Software Licenses certificate, installer and corresponding certificate of completion and acceptance from MISS-SAD.

8. Non-Graft Clause
8.1. The winning Vendor warrants that it has not given nor promised to give any money or gift to any officer or employee of the BTr, or any member of the Bids and Awards Committee (BAC), BAC Secretariat or TWG, to secure this contract.

9. Vendor Requirements
9.1. The Vendor must have at least FIVE (5) YEARS existence in IT Business.
9.2. The Vendor must be a Certified Partner for the product being offered.
9.3. The Vendor must have certified Support Engineer for the product and brand being offered.
9.4. The Vendor must be actively registered in the PhilGEPS.
9.5. The Vendor must have completed similar project in the last three (3) years.
9.6. The Vendor must have completed single similar contract amounting to at least 50% of the ABC.
9.7. Joint Venture is not allowed.

**Line Items**

| Item No. | Product/Service Name | Description | Quantity | UOM | Budget (PHP) |
|---|---|---|---|---|---|
| 1 | PROVISION OF ANTIVIRUS SOFTWARE FOR VARIOUS SERVER | PROVISION OF ANTIVIRUS SOFTWARE FOR VARIOUS SERVER ASSETS OF THE BUREAU OF THE TREASURY | 1 | Lot | 970,000.00 |

| | |
|---|---|
| **Created by** | Mr. Clarence Bolante Bunan |
| **Date Created** | 05/11/2018 |