



# PhilGEPS

Philippine Government Electronic Procurement System

Central Portal for  
Philippine Government  
Procurement Opportunities

[Help](#)

## Bid Notice Abstract

### Request for Quotation (RFQ)

**Reference Number** 10065264  
**Procuring Entity** MARITIME INDUSTRY AUTHORITY (MARINA)  
**Title** PROCUREMENT OF ANTI-VIRUS SUBSCRIPTION  
**Area of Delivery** Metro Manila

<b>Solicitation Number:</b>	2023-07-325	<b>Status</b>	<b>Pending</b>
<b>Trade Agreement:</b>	Implementing Rules and Regulations		
<b>Procurement Mode:</b>	Negotiated Procurement - Small Value Procurement (Sec. 53.9)	<b>Associated Components</b>	1
<b>Classification:</b>	Goods - General Support Services	<b>Bid Supplements</b>	0
<b>Category:</b>	Information Technology	<b>Document Request List</b>	0
<b>Approved Budget for the Contract:</b>	PHP 320,000.00		
<b>Delivery Period:</b>	2 Year/s		
<b>Client Agency:</b>			
<b>Contact Person:</b>	ATTY. SHARON L. DE CHAVEZ - ALEDO The BAC Chairperson c/o BAC Office, 10th Floor, MARINA Bldg. A. Bonifacio Drive cor. 20th Street, Port Area Manila Metro Manila Philippines 1018 63-2-85246518  bacsec@marina.gov.ph	<b>Date Published</b>	24/08/2023
		<b>Last Updated / Time</b>	23/08/2023 11:07 AM
		<b>Closing Date / Time</b>	30/08/2023 12:00 PM
<b>Description</b>  PROCUREMENT OF ANTI-VIRUS SUBSCRIPTION  Please see attached files or you may visit <a href="https://marina.gov.ph/small-value-procurement/">https://marina.gov.ph/small-value-procurement/</a>  All submission in response to the RFQ shall be in hard copy with fresh signature only. Submission in electronic copies shall not be entertained.			

**Created by** ATTY. SHARON L. DE CHAVEZ - ALEDO  
**Date Created** 22/08/2023

The PhilGEPS team is not responsible for any typographical errors or misinformation presented in the system. PhilGEPS only displays information provided for by its clients, and any queries regarding the postings should be directed to the contact person/s of the concerned party.



REPUBLIC OF THE PHILIPPINES  
DEPARTMENT OF TRANSPORTATION  
MARITIME INDUSTRY AUTHORITY

**REQUEST FOR QUOTATION**

DATE: \_\_\_\_\_

Name of Company : \_\_\_\_\_

Address : \_\_\_\_\_

Business Permit Number : \_\_\_\_\_

Company TIN : \_\_\_\_\_

PhilGEPS Registration Number (required): \_\_\_\_\_

Name of Representative & Designation : \_\_\_\_\_

The **Maritime Industry Authority (MARINA)** through its Bids and Awards Committee (BAC), intends to procure **Anti-Virus Subscription** in accordance with Section 53.9 (Small Value Procurement) of the 2016 Revised Implementing Rules and Regulations of Republic Act No. 9184. The Approved Budget for the Contract (ABC) is **Three Hundred Twenty Thousand Pesos (320,000.00)**, inclusive of all applicable government charges. The period for the performance of the obligations shall not go beyond of the appropriations for this Procurement Project.

Please quote your **best offer** for the item/s described herein, **subject to the Terms and Conditions** provided at the last page of this Request for Quotation (RFQ). Submit your quotation duly signed by your representative **not later than 30 August 2023** at the MARINA BAC Office located at 10<sup>th</sup> Floor MARINA Building, Bonifacio Drive cor., 20<sup>th</sup> Street, Port Area, Manila, Philippines.

A copy of your **Valid Business/Mayor's Permit, PhilGEPS Registration, Omnibus Sworn Statement** (accompanied by the duly notarized Special Power of Attorney, Board/Partnership Resolution, or Secretary's Certificate, whichever is applicable), and **Proof of Qualification of the Supplier** are required to be submitted along with your signed quotation/proposal.

For any clarification, you may contact Ms. Ellerie Torrente or Ms. Kristen Nicole Velasco at telephone no. **(+632) 8524-6518** or email address at **[bacsec@marina.gov.ph](mailto:bacsec@marina.gov.ph)**

  
ATTY. SHARON D. ALEJO  
BAC Chairperson

**INSTRUCTIONS:**

- (1) Accomplish this RFQ correctly and accurately.
- (2) Do not alter the content of this form in any way.
- (3) All technical specifications are mandatory. Failure to comply with any of the mandatory requirements will disqualify your quotation.
- (4) Failure to follow these instructions will disqualify your entire quotation.

Supplier's must state here either "**Comply**" or **any equivalent term** in the column "Supplier's Statement of Compliance" against each of the individual parameters of each specification. Please quote your **best offer** for the item/s below. Please do not leave any blank items. Indicate "**0**" if item being offered is for free.

After having carefully read and accepted the Terms and Conditions in the Request for Quotation, hereunder is our quotation for the item/s as follows:

Item No.	Description/Technical Specifications	Supplier's Statement of Compliance	Unit Cost (VAT inclusive)	Total Cost (VAT inclusive)
1 LOT	<b>300 ANTI-VIRUS SUBSCRIPTION FOR THE PERIOD OF TWO (2) YEARS</b>			
	<b>Technical Specifications:</b> <b>A. File Anti-Virus &amp; Anti-Malware</b>  1. Dedicated engine for Ransomware detection and blocking. 2. Ransomware protection must have the following checking process: <ul style="list-style-type: none"><li>o Reserve check</li><li>o Behavioral check</li><li>o Resources check</li><li>o Signature check</li><li>o File check</li></ul> 3. Patented scanning and detection technology for virus and malwares. 4. Protection for Windows at the WinSock layer, scanning thru WinSock Layer scan before it reaches to the operating system. 5. Scheduled and On-demand Scanning 6. Configurable scanning priority (high, medium, and low) 7. Configurable to set background scanning 8. Customizable actions on malware of infected file (clean, quarantine, and delete) 9. Ability to block attachments on Instant Messengers 10. Website that capable to upload and analyze potential malware or virus			



	<p><b>B. Mail Anti-Virus &amp; Anti-Spam Protection</b></p> <ol style="list-style-type: none"> <li>1. Incoming and outgoing emails scanning for spam and phishing emails with artificial intelligence and machine learning support.</li> <li>2. Scanning must cover standard and SSL mail ports.</li> <li>3. Support for the following filtering layers: <ul style="list-style-type: none"> <li>o Customizable word/phrase filtering</li> <li>o Mail Non-Intrusive Learning Pattern</li> <li>o Email Header and X-Spam Rules Checking</li> <li>o SPF Checking</li> <li>o SURBL &amp; RBL (pre-defined and customizable) checking</li> </ul> </li> <li>4. Blocking of attachments based on type (pre-defined and customizable with wildcard support)</li> <li>5. Archival of Mail and Attachments with archived mail viewer.</li> <li>6. Product should be able to take actions on malicious emails based on user defined actions.</li> <li>7. Customizable alert notifications for various level of events in like of virus outbreak and data theft.</li> <li>8. Customizable actions for spam/phishing emails.</li> <li>9. Able to tag spam mails in subject line with SPAM for considered spam mails.</li> </ol>			
--	--	--	--	--

	<p><b>C. Mail Gateway Anti-Spam and Content Security</b></p> <ol style="list-style-type: none"> <li>1. Scans all the emails in Real-time for Viruses, Worms, Trojans, Adware and hidden malicious content using powerful heuristic driven Dual Anti-virus engines</li> <li>2. Non-Intrusive Learning Pattern (NILP) - is an advanced spam filtering method with the intelligence which analyzes and classify each mail as spam or ham according to the user's behavioral patterns</li> <li>3. DKIM and DMARC Support</li> <li>4. Can filter out Image Spam</li> <li>5. Greylisting</li> <li>6. Customizable options to archive emails and attachments flowing in and out of system with comprehensive content auditing</li> <li>7. Scans all incoming and outgoing emails in real-time for offensive words and adult content with the help of Security Policies</li> <li>8. Provides advanced analytical reports in graphical and nongraphical formats</li> <li>9. Limit the outgoing email traffic by controlling the number of emails and recipients that any individual can send within specified time period</li> <li>10. Powered with LDAP and POP3 Authenticated Web Administration</li> <li>11. Attachments having file extensions such as EXE, COM, CHM or BAT can be blocked from being sent or received</li> </ol>			
	<p><b>D. Web Protection</b></p> <ol style="list-style-type: none"> <li>1. Capable to allow and block URL or website access based on database of predefined category or end-user customized category</li> <li>2. Allow and block URL or website access based on scheduled time</li> <li>3. Product should be able to allow customized web security policies in per user and per group</li> <li>4. Easy configuration for block all sites with allowed particular websites only</li> <li>5. Anti-phishing filter for websites based in intelligent heuristics</li> <li>6. Product should have cloud intelligence capabilities for understanding and blocking malicious URLs</li> </ol>			

<p><b>E. Device and Application Control</b></p> <ol style="list-style-type: none"> <li>1. Password protection for USB removable devices.</li> <li>2. Password protection for the uninstallation of the endpoint security.</li> <li>3. Capability to keep a copy of files copied from endpoint to external storage device and vice versa.</li> <li>4. Configurable to allow or block CD/DVD Drives, Web Cam, External Storage and any USB devices.</li> <li>5. USB Vaccination Tool for USB Storage Devices.</li> <li>6. Application Control: Whitelisting and blacklisting of application which are only allowed by the administrator.</li> <li>7. Time-based Application Restriction.</li> </ol>			
<p><b>F. Privacy Protection and Maintenance</b></p> <ol style="list-style-type: none"> <li>1. Integrated virtual keyboard for key logger evasion.</li> <li>2. Ability to clear the following: <ul style="list-style-type: none"> <li>o Temporary internet and windows temporary files</li> <li>o Remove temp files, cookies, MRU lists from registry</li> <li>o Browser history based on a schedule</li> <li>o Clear cache, cookies, plugins ActiveX, and history on a schedule.</li> </ul> </li> </ol>			
<p><b>G. Rescue and Recovery Utilities</b></p> <ol style="list-style-type: none"> <li>1. Rescue Disc: Rescue mode boot option so that scanning is possible without loading the installed OS</li> <li>2. Rescue USB: Linux-based Rescue USB for cleaning of rootkits and file infectors</li> <li>3. Secure Delete: Functionality to delete a certain data marked by user in such way that any other 3rd party software's should not be able to recover it.</li> <li>4. Backup tool with encryption functionality for additional security</li> </ol>			

	<p><b>H. User Defined File and Folder Protection (Network Protection)</b></p> <ol style="list-style-type: none"> <li>1. Data leakage protection function which data can be marked for protection against access and modification over network</li> <li>2. Protection against attack or threats on network via lateral movement.</li> <li>3. Centrally managed server via console and on heterogeneous platform (Windows, Linux, &amp; MacOS)</li> <li>4. Real-time dashboard on the status of the endpoints (installed, updated, outdated)</li> <li>5. Report Generation of the following: <ul style="list-style-type: none"> <li>o Installed count</li> <li>o Not Installed Count</li> <li>o Updated non-updated</li> <li>o Top 10 infected computers</li> <li>o Asset Changes</li> <li>o Top Exploit Blocked</li> </ul> </li> <li>6. System Actions List of the following: <ul style="list-style-type: none"> <li>o Lock</li> <li>o Log off</li> <li>o Shutdown</li> <li>o Restart</li> </ul> </li> <li>7. Policy deployment based on per user and per group</li> <li>8. Auto-grouping for managed workstations</li> <li>9. Remote application silent installation</li> <li>10. Configurable FTP and HTTP update source</li> <li>11. QoS configuration for workstations</li> <li>12. Role based administrative access</li> <li>13. One-time password facility for temporary administrator access with time duration settings.</li> <li>14. Outbreak notification thru email based on configurable threshold</li> <li>15. Integration with 3rd party CRM via SNMP</li> <li>16. Administrator broadcast messaging</li> <li>17. Active Directory/LDAP Synchronization</li> <li>18. Scheduled Task Deployment</li> <li>19. Child server (branch update server) for the branches will download policies and updates from the central server and distribute to branch workstations to reduce bandwidth consumption.</li> <li>20. Live status Online and offline workstations</li> </ol>			
--	---	--	--	--

<b>I. Reporting</b> <ol style="list-style-type: none"> <li>1. Monitors and logs printing task done by all managed computers</li> <li>2. Monitors and logs the file activity of the managed computers.</li> <li>3. Monitors and logs the session activity of the managed computers.</li> <li>4. Ability to generate reports to *.html, *.xls, *.pdf.</li> <li>5. Report Generation by weekly and monthly.</li> </ol>			
<b>J. Asset Management and Patch Management</b> <ol style="list-style-type: none"> <li>1. Integrated asset management: <ul style="list-style-type: none"> <li>o Software and Hardware Inventory</li> <li>o License Inventory</li> <li>o Hardware changes</li> <li>o Application Installed</li> </ul> </li> <li>2. Workstation software/hardware modification alerts and reports.</li> <li>3. Ability to generate reports to *.html, *.xls, *.pdf for the asset inventory.</li> <li>4. Capability to check critical patches installed on workstation and able to push critical updates on workstation.</li> <li>5. Capability to display windows security patches</li> </ol>			
<b>K. Certifications</b> <ol style="list-style-type: none"> <li>1. VB 100 Virus Definition</li> <li>2. AV Test</li> <li>3. AV Comparatives</li> </ol>			



	<b>L. Operating Systems Supported</b>  1. Clients - Workstation Operating System <b>Windows:</b> XP SP 2 / Vista / Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / 2000 (Workstation) [All 32-bit and 64-bit Editions] 2. Server- Server Class OS <b>Windows:</b> 2019 / 2016 / 2012 / SBS 2011 / Essential / 2008 R2 / 2008 / 2003 R2 / 2003 / 2000 [All 32-bit and 64-bit Editions] 3. <b>Linux:</b> RHEL 4 and above / CentOS 5.10 and above / SLES 10 SP3 and above / Debian 4.0 and above / openSuSe 10.1 and above / Fedora 5.0 and above /Ubuntu 6.06 and above [All 32-bit and 64-bit Editions] 4. <b>MacOS:</b> OS X Snow Leopard (10.6 or later) / OS X Lion (10.7 or later) / OS X Mountain Lion (10.8 or later) / OS X Mavericks (10.9 or later)/ OS X Yosemite (10.10 or later) / OS X El Capitan (10.11 or later) / macOS Sierra (10.12 or later)/ macOS High Sierra (10.13 or later)			
--	---	--	--	--

\_\_\_\_\_  
Signature over Printed Name

\_\_\_\_\_  
Position/Designation

\_\_\_\_\_  
Office Telephone No.

\_\_\_\_\_  
Fax/Mobile No.

\_\_\_\_\_  
Email Address/es

## **SCHEDULE OF REQUIREMENTS**

The delivery schedule expressed as week/months stipulates hereafter a delivery date, which is the date to the project site.

<b>Item No.</b>	<b>Description</b>	<b>Delivery Schedule</b>	<b>Supplier's Statement of Compliance</b>
	<b>300 ANTI-VIRUS SUBSCRIPTION</b>	Required to be delivered and deployed within thirty (30) calendar days upon Receipt of Notice to Proceed.	
	<b>Technical Support</b> <ol style="list-style-type: none"> <li>1. The Bidder is required to Install the and Technical Training</li> <li>2. The Bidder is required to provide assistance through telephone, electronic mail and onsite visits to resolve technical and other related issued on weekdays, commencing from 8:00 am till 5:00 pm.</li> <li>3. The Bidder must provide a monthly health check during the subscription period to ensure that the product is properly working</li> </ol>		
	<b>Qualification of The Supplier:</b> <ul style="list-style-type: none"> <li>- The supplier must be legally registered, has at least 3 years' experience in supplying anti-virus solutions and should submit at least two (2) Client Satisfactory Certificates for the last two (2) year</li> </ul>	Required to be submitted along with your signed quotation/ proposal	
	<b>Other Documentary Requirements:</b> <ul style="list-style-type: none"> <li>- <b>Valid Business/Mayor's Permit</b></li> <li>- <b>PhilGEPS Registration</b></li> <li>- <b>Omnibus Sworn Statement</b> (accompanied by the duly notarized Special Power of Attorney, Board/Partnership Resolution, or Secretary's Certificate, whichever is applicable)</li> </ul>		

\_\_\_\_\_  
Signature over Printed Name

\_\_\_\_\_  
Position/Designation

\_\_\_\_\_  
Office Telephone No.

\_\_\_\_\_  
Fax/Mobile No.

\_\_\_\_\_  
Email Address/es

<b><u>FINANCIAL OFFER</u></b>	
<b>Approved Budget for the Contract</b>	<b>Total Offered Quotation</b>
<p style="text-align: center;"><b>THREE HUNDRED TWENTY THOUSAND PESOS</b></p> <p style="text-align: center;"><b>(P320,000.00)</b></p>	<p>In words: _____</p> <p>_____</p> <p>_____</p> <p>_____</p> <p>In figures: _____</p> <p>_____</p> <p>_____</p> <p>_____</p>

<b>Terms of Payment:</b>	<p>Payment shall be made thirty (30) days upon the receipt of the Billing Statement and Accomplishment Report on a Bank-to-Bank basis.</p> <p>In case of Automatic Debit Arrangement (ADA) through Land Bank of the Philippines (LBP) facilities, or other Commercial Banks, the applicable bank charges shall be for the account of the supplier. The supplier shall submit bank details together with billing statement/ invoice for ready reference.</p>
Banking Institution:	
Account Number:	
Account Name:	
Branch:	

\_\_\_\_\_  
Signature over Printed Name

\_\_\_\_\_  
Position/Designation

\_\_\_\_\_  
Office Telephone No.

\_\_\_\_\_  
Fax/Mobile No.

\_\_\_\_\_  
Email Address/es

### **TERMS AND CONDITIONS:**

1. Bidders shall provide correct and accurate information required in this form.
2. Price quotation/s must be valid for a period of *thirty (30) calendar days* from the date of submission.
3. Price quotation, denominated in Philippine peso, shall include all taxes, duties and/or other charges payable relative to the items described in the RFQ.
4. Quotations exceeding the Approved Budget for the Contract shall be rejected.
5. **All submission in response to the RFQ shall be in hard copy with fresh signature only. Submission in electronic copies shall not be entertained.**
6. Award of contract shall be made to lowest calculated and responsive quotation (for goods and infrastructure) or, the highest rated offer (for consulting services) which complies with the minimum technical specifications and other terms and conditions stated herein.
7. Any interlineations, erasures or overwriting shall be valid only if they are signed or initialed by you or any of your duly authorized representative/s.
8. The item/s shall be delivered according to the requirements specified in the Technical Specifications.
9. The MARINA shall have the right to inspect and/or to test the goods to confirm their conformity to the technical specifications.
10. In case two or more bidders are determined to have submitted the Lowest Calculated Quotation/Lowest Calculated and Responsive Quotation, the MARINA-BAC shall adopt and employ "draw lots" as the tie-breaking method to finally determine the single winning provider in accordance with GPPB Circular 06-2005.
11. **Payment shall be processed after delivery and upon the submission of the required supporting documents, in accordance with existing accounting rules and regulations. Please note that the corresponding bank transfer fee, if any, shall be chargeable to the supplier's account.**
12. Liquidated damages equivalent to one tenth of one percent (0.1%) of value of the goods not delivered within the prescribed delivery period shall be imposed per day of delay. The MARINA shall rescind the contract once the cumulative amount of liquidated damages reaches ten percent (10%) of the amount of the contract without prejudice to other courses of action and remedies open to it.

---

Signature over Printed Name

---

Position/Designation

## **TERMS OF REFERENCE**

### **ANTI-VIRUS SUBSCRIPTION**

#### **I. Approved Budget Contract**

The supplier shall bid for all items described in this Terms of reference, which shall not exceed the Approved Budget Contract (ABC) in the amount of Three Hundred Twenty-Thousand Pesos (320,000.00), inclusive of all applicable government charges.

#### **II. Number of Subscription**

1. 300 /

#### **III. Technical Specification**

##### **A. File Anti-Virus & Anti-Malware**

1. Dedicated engine for **Ransomware** detection and blocking.
2. Ransomware protection must have the following checking process:
  - o Reserve check
  - o Behavioral check
  - o Resources check
  - o Signature check
  - o File check
3. Patented scanning and detection technology for virus and malwares.
4. Protection for Windows at the WinSock layer, scanning thru WinSock Layer scan before it reaches to the operating system.
5. Scheduled and On-demand Scanning
6. Configurable scanning priority (high, medium, and low)
7. Configurable to set background scanning
8. Customizable actions on malware of infected file (clean, quarantine, and delete)
9. Ability to block attachments on Instant Messengers
10. Website that capable to upload and analyze potential malware or virus

##### **B. Mail Anti-Virus & Anti-Spam Protection**

1. Incoming and outgoing emails scanning for spam and phishing emails with artificial intelligence and machine learning support.
2. Scanning must cover standard and SSL mail ports.
3. Support for the following filtering layers:
  - o Customizable word/phrase filtering
  - o Mail Non-Intrusive Learning Pattern
  - o Email Header and X-Spam Rules Checking
  - o SPF Checking
  - o SURBL & RBL (pre-defined and customizable) checking
4. Blocking of attachments based on type (pre-defined and customizable with





wildcard support)

5. Archival of Mail and Attachments with archived mail viewer.
6. Product should be able to take actions on malicious emails based on user defined actions.
7. Customizable alert notifications for various level of events in like of virus outbreak and data theft.
8. Customizable actions for spam/phishing emails.
9. Able to tag spam mails in subject line with SPAM for considered spam mails.

### **C. Mail Gateway Anti-Spam and Content Security**

1. Scans all the emails in Real-time for Viruses, Worms, Trojans, Adware and hidden malicious content using powerful heuristic driven Dual Anti-virus engines
2. Non-Intrusive Learning Pattern (NILP) - is an advanced spam filtering method with the intelligence which analyzes and classify each mail as spam or ham according to the user's behavioral patterns
3. DKIM and DMARC Support
4. Can filter out Image Spam
5. Greylisting
6. Customizable options to archive emails and attachments flowing in and out of system with comprehensive content auditing
7. Scans all incoming and outgoing emails in real-time for offensive words and adult content with the help of Security Policies
8. Provides advanced analytical reports in graphical and nongraphical formats
9. Limit the outgoing email traffic by controlling the number of emails and recipients that any individual can send within specified time period
10. powered with LDAP and POP3 Authenticated Web Administration
11. Attachments having file extensions such as EXE, COM, CHM or BAT can be blocked from being sent or received

### **D. Web Protection**

1. Capable to allow and block URL or website access based on database of pre-defined category or end-user customized category
2. Allow and block URL or website access based on scheduled time
3. Product should be able to allow customized web security policies in per user and per group
4. Easy configuration for block all sites with allowed particular websites only
5. Anti-phishing filter for websites based in intelligent heuristics
6. Product should have cloud intelligence capabilities for understanding and blocking malicious URLs



## **E. Device and Application Control**

1. Password protection for USB removable devices.
2. Password protection for the uninstallation of the endpoint security.
3. Capability to keep a copy of files copied from endpoint to external storage device and vice versa.
4. Configurable to allow or block CD/DVD Drives, Web Cam, External Storage and any USB devices.
5. USB Vaccination Tool for USB Storage Devices.
6. Application Control: Whitelisting and blacklisting of application which are only allowed by the administrator.
7. Time-based Application Restriction.

## **F. Privacy Protection and Maintenance**

1. Integrated virtual keyboard for key logger evasion.
2. Ability to clear the following:
  - o Temporary internet and windows temporary files
  - o Remove temp files, cookies, MRU lists from registry
  - o Browser history based on a schedule
  - o Clear cache, cookies, plugins ActiveX, and history on a schedule.

## **G. Rescue and Recovery Utilities**

1. Rescue Disc: Rescue mode boot option so that scanning is possible without loading the installed OS
2. Rescue USB: Linux-based Rescue USB for cleaning of rootkits and file infectors
3. Secure Delete: Functionality to delete a certain data marked by user in such way that any other 3rd party software's should not be able to recover it.
4. Backup tool with encryption functionality for additional security

## **H. User Defined File and Folder Protection (Network Protection)**

1. Data leakage protection function which data can be marked for protection against access and modification over network
2. Protection against attack or threats on network via lateral movement.
3. Centrally managed server via console and on heterogeneous platform (Windows, Linux, & MacOS)
4. Real-time dashboard on the status of the endpoints (installed, updated, outdated)
5. Report Generation of the following:
  - o Installed count
  - o Not Installed Count
  - o Updated non-updated





- o Top 10 infected computers
- o Asset Changes
- o Top Exploit Blocked
- 6. System Actions List of the following:
  - o Lock
  - o Log off
  - o Shutdown
  - o Restart
- 7. Policy deployment based on per user and per group
- 8. Auto-grouping for managed workstations
- 9. Remote application silent installation
- 10. Configurable FTP and HTTP update source
- 11. QoS configuration for workstations
- 12. Role based administrative access
- 13. One-time password facility for temporary administrator access with time duration settings.
- 14. Outbreak notification thru email based on configurable threshold
- 15. Integration with 3rd party CRM via SNMP
- 16. Administrator broadcast messaging
- 17. Active Directory/LDAP Synchronization
- 18. Scheduled Task Deployment
- 19. Child server (branch update server) for the branches will download policies and updates from the central server and distribute to branch workstations to reduce bandwidth consumption.
- 20. Live status Online and offline workstations

## **I. Reporting**

1. Monitors and logs printing task done by all managed computers
2. Monitors and logs the file activity of the managed computers.
3. Monitors and logs the session activity of the managed computers.
4. Ability to generate reports to \*.html, \*.xls, \*.pdf.
5. Report Generation by weekly and monthly.

## **J. Asset Management and Patch Management**

1. Integrated asset management
  - o Software and Hardware Inventory
  - o License Inventory
  - o Hardware changes
  - o Application Installed
2. Workstation software/hardware modification alerts and reports.
3. Ability to generate reports to \*.html, \*.xls, \*.pdf for the asset inventory.
4. Capability to check critical patches installed on workstation and able to push critical updates on workstation.
5. Capability to display windows security patches

## **K. Certifications**

1. VB 100 Virus Definition
2. AV Test
3. AV Comparatives

## **L. Operating Systems Supported**

1. Clients - Workstation Operating System  
**Windows:** XP SP 2 / Vista / Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / 2000 (Workstation) [All 32-bit and 64-bit Editions]
2. Server- Server Class OS  
**Windows:** 2019 / 2016 / 2012 / SBS 2011 / Essential / 2008 R2 / 2008 / 2003 R2 / 2003 / 2000 [All 32-bit and 64-bit Editions]
3. **Linux:** RHEL 4 and above / CentOS 5.10 and above / SLES 10 SP3 and above / Debian 4.0 and above / openSuSe 10.1 and above / Fedora 5.0 and above / Ubuntu 6.06 and above [All 32-bit and 64-bit Editions]
4. **MacOS:** OS X Snow Leopard (10.6 or later) / OS X Lion (10.7 or later) / OS X Mountain Lion (10.8 or later) / OS X Mavericks (10.9 or later) / OS X Yosemite (10.10 or later) / OS X El Capitan (10.11 or later) / macOS Sierra (10.12 or later) / macOS High Sierra (10.13 or later)

## **IV. Delivery**

The winning bidder is required to deliver and deploy the solution within 30 calendar days after issuance of Notice to Proceed.

## **V. Technical Support**

1. The Bidder is required to Install the and Technical Training
2. The Bidder is required to provide assistance through telephone, electronic mail and onsite visits to resolve technical and other related issued on weekdays, commencing from 8:00 am till 5:00 pm.
3. The Bidder must provide a monthly health check during the subscription period to ensure that the product is properly working

## **VI. Qualification of the Supplier**

- The supplier must be legally registered, has at least 3 years' experience in supplying anti-virus solutions and should submit at least two (2) Client Satisfactory Certificates for the last two (2) years.



## VI. Payment

- The payment can be made one-time fee annually upon issuance of the Billing Statement on a Bank-to-bank basis. Automatic Debit Arrangement (ADA) through Land Bank of the Philippines (LBP) facilities, for other Commercial Bank, applicable bank charges shall be for the account of supplier. The supplier shall submit bank details together with billing statement/ invoice for ready reference.


Prepared by:

  
**DALMACIO L. GONZALES JR.**  
Chief, ICTMD

Recommending Approval:

  
**SAMUEL L. BATALLA**  
Executive Director  
STCW Office

Reviewed by:

  
**JOHN E. GUARDAYA**  
Head, TWG for IT

  
**Atty. SHARON D. ALEDO**  
Chairperson, MARINA BAC

APPROVED / DISAPPROVED:

  
**Atty. HERNANI N. FABIA**  
Administrator  
DATE SO# 2023-282

Version 1  
July 14, 2023



**MARITIME INDUSTRY AUTHORITY**

Item No.	Unit	Item Description	Quantity	Unit Cost	Total Cost
		ANTI-VIRUS SUBSCRIPTION	1	320,000.00	320,000.00
*****	*****	*****	*****	*****	***** ***
<div style="border: 1px solid black; padding: 5px; display: inline-block;">           WITH SUPPLEMENTAL TO PPMP            FY: <u>2015</u> </div>					

**Note:**

## Omnibus Sworn Statement (Revised)

*[shall be submitted with the Bid]*

REPUBLIC OF THE PHILIPPINES )  
CITY/MUNICIPALITY OF \_\_\_\_\_ ) S.S.

### AFFIDAVIT

I, [Name of Affiant], of legal age, [Civil Status], [Nationality], and residing at [Address of Affiant], after having been duly sworn in accordance with law, do hereby depose and state that:

1. *[Select one, delete the other:]*

*[If a sole proprietorship:]* I am the sole proprietor or authorized representative of [Name of Bidder] with office address at [address of Bidder];

*[If a partnership, corporation, cooperative, or joint venture:]* I am the duly authorized and designated representative of [Name of Bidder] with office address at [address of Bidder];

2. *[Select one, delete the other:]*

*[If a sole proprietorship:]* As the owner and sole proprietor, or authorized representative of [Name of Bidder], I have full power and authority to do, execute and perform any and all acts necessary to participate, submit the bid, and to sign and execute the ensuing contract for [Name of the Project] of the [Name of the Procuring Entity], as shown in the attached duly notarized Special Power of Attorney;

*[If a partnership, corporation, cooperative, or joint venture:]* I am granted full power and authority to do, execute and perform any and all acts necessary to participate, submit the bid, and to sign and execute the ensuing contract for [Name of the Project] of the [Name of the Procuring Entity], as shown in the attached [state title of attached document showing proof of authorization (e.g., duly notarized Secretary's Certificate, Board/Partnership Resolution, or Special Power of Attorney, whichever is applicable)];

3. [Name of Bidder] is not "blacklisted" or barred from bidding by the Government of the Philippines or any of its agencies, offices, corporations, or Local Government Units, foreign government/foreign or international financing institution whose blacklisting rules have been recognized by the Government Procurement Policy Board, by itself or by relation, membership, association, affiliation, or controlling interest with another blacklisted person or entity as defined and provided for in the Uniform Guidelines on Blacklisting;

4. Each of the documents submitted in satisfaction of the bidding requirements is an authentic copy of the original, complete, and all statements and information provided therein are true and correct;

5. [Name of Bidder] is authorizing the Head of the Procuring Entity or its duly authorized representative(s) to verify all the documents submitted;

6. *[Select one, delete the rest:]*

*[If a sole proprietorship:]* The owner or sole proprietor is not related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), the Technical



Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

*[If a partnership or cooperative:]* None of the officers and members of *[Name of Bidder]* is related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

*[If a corporation or joint venture:]* None of the officers, directors, and controlling stockholders of *[Name of Bidder]* is related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

7. *[Name of Bidder]* complies with existing labor laws and standards; and
8. *[Name of Bidder]* is aware of and has undertaken the responsibilities as a Bidder in compliance with the Philippine Bidding Documents, which includes:
  - a. Carefully examining all of the Bidding Documents;
  - b. Acknowledging all conditions, local or otherwise, affecting the implementation of the Contract;
  - c. Making an estimate of the facilities available and needed for the contract to be bid, if any; and
  - d. Inquiring or securing Supplemental/Bid Bulletin(s) issued for the *[Name of the Project]*.
9. *[Name of Bidder]* did not give or pay directly or indirectly, any commission, amount, fee, or any form of consideration, pecuniary or otherwise, to any person or official, personnel or representative of the government in relation to any procurement project or activity.
10. In case advance payment was made or given, failure to perform or deliver any of the obligations and undertakings in the contract shall be sufficient grounds to constitute criminal liability for Swindling (Estafa) or the commission of fraud with unfaithfulness or abuse of confidence through misappropriating or converting any payment received by a person or entity under an obligation involving the duty to deliver certain goods or services, to the prejudice of the public and the government of the Philippines pursuant to Article 315 of Act No. 3815 s. 1930, as amended, or the Revised Penal Code.

IN WITNESS WHEREOF, I have hereunto set my hand this \_\_\_ day of \_\_\_, 20\_\_ at \_\_\_\_\_, Philippines.

*[Insert NAME OF BIDDER OR ITS AUTHORIZED REPRESENTATIVE]*

*[Insert signatory's legal capacity]*  
Affiant

***[Jurat]***

*[Format shall be based on the latest Rules on Notarial Practice]*