



Bid Notice Abstract

Request for Quotation (RFQ)

Reference Number 7938942
Procuring Entity MARITIME INDUSTRY AUTHORITY (MARINA)
Title SUPPLY, DELIVERY, INSTALLATION AND CONFIGURATION OF FIVE HUNDRED (500) CORPORATE ANTIVIRUS LICENSE WITH HYBRID NETWORK SUPPORT (2 YEAR SUBSCRIPTION)
Area of Delivery Metro Manila

Solicitation Number:	2021-07-304	Status	Pending
Trade Agreement:	Implementing Rules and Regulations		
Procurement Mode:	Negotiated Procurement - Small Value Procurement (Sec. 53.9)	Associated Components	1
Classification:	Goods		
Category:	Information Technology Parts & Accessories & Perip	Bid Supplements	0
Approved Budget for the Contract:	PHP 500,000.00		
Delivery Period:	30 Day/s	Document Request List	0
Client Agency:			
Contact Person:	VADM Rene V. Medina AFP (Ret) The BAC Chairperson MARINA Building, A. Bonifacio Drive corner 20th St Port Area, Manila Manila Metro Manila Philippines 1018 63-2-85246518 63-2-85246518 2021marinabac@gmail.com	Date Published	21/08/2021
		Last Updated / Time	20/08/2021 08:58 AM
		Closing Date / Time	24/08/2021 13:00 PM

Description

SUPPLY, DELIVERY, INSTALLATION AND CONFIGURATION OF FIVE HUNDRED (500) CORPORATE ANTIVIRUS LICENSE WITH HYBRID NETWORK SUPPORT (2 YEAR SUBSCRIPTION)

Please see attached file.

You may visit our website at marina.gov.ph (under transparency tab)

Created by VADM Rene V. Medina AFP (Ret)
Date Created 20/08/2021

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

The Maritime Industry Authority (MARINA) – Bids and Awards Committee (BAC), will undertake a Small Value Procurement for the **SUPPLY, DELIVERY, INSTALLATION AND CONFIGURATION OF FIVE HUNDRED (500) CORPORATE ANTIVIRUS LICENSE WITH HYBRID NETWORK SUPPORT (2 YEAR SUBSCRIPTION)** for FY 2021 in accordance with Section 53.9 of the 2016 Revised Implementing Rules and Regulation of Republic Act No. 9184

Please quote your **best offer** for the item 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 you or your representative **not later than (24 August 2021 , 01:00 P.M.)** at the MARINA BAC Office, located at 10th Floor MARINA Building, Bonifacio Drive cor. 20th Street, Port Area, Manila, Philippines.

A copy of your **2021 Business/Mayor's Permit¹** (at least 3 years experience in supplying anti-virus solutions), **PhilGEPS Registration Number, Latest Income Tax Return, and Omnibus Sworn Statement²** are required to be submitted along with your quotation/proposal.

Additional MARINA requirements to be submitted, a **brochure/datasheet of proposed Anti-Virus Solution** and **submit atleast two (2) Client Satisfactory Certificates issued in the last two (2) years**

For any clarification, you may contact us at 2021marinabac@gmail.com.

VADM RENE V MEDINA AFP (RET)
MARINA BAC Chairperson

¹ In case of recently expired Mayor's/Business permit, it shall be accepted together with its official receipt as proof that the bidder has applied for renewal within the period prescribed by the concerned local government unit, provided that the renewed permit shall be submitted after award of contract but before payment in accordance with item 6.2 of Government Procurement Policy Board (GPPB) Resolution No. 09-2020.

² In case of Unnotarized Omnibus Sworn Statement, it shall be accepted, provided that the notarized Omnibus Sworn Statement shall be submitted after award of contract but before payment in accordance with item 6.3 of GPPB No. 09-2020.

DATE: _____

NAME OF COMPANY:

ADDRESS:

COMPANY ADDRESS:

COMPANY TIN NUMBER:

PHILGEPS REGISTRATION NUMBER:

NAME OF REPRESENTATIVE & DESIGNATION:

MARINA Building
20th Street corner Bonifacio Drive
1018 Port Area (South), Manila

Tel. Nos: (632) 523-9078 / 526-0971
Fax No: (632) 524-2895
Website: www.marina.gov.ph

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.

Bidder's must state here either "Comply" or any equivalent term in the column "Bidder's Statement of Compliance" against each of the individual parameters of each specification.

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:

SUPPLY, DELIVERY, INSTALLATION AND CONFIGURATION OF FIVE HUNDRED (500) CORPORATE ANTIVIRUS LICENSE WITH HYBRID NETWORK SUPPORT (2 YEAR SUBSCRIPTION)		
Code	Technical Specification	Bidder's Statement of Compliance
A	FILE ANTI-VIRUS & ANTI-MALWARE <ol style="list-style-type: none">1. Dedicated engine for Ransomware detection and blocking.2. Ransomware protection must have the following checking process:<ol style="list-style-type: none">a. Reserve checkb. Behavioral checkc. Resources checkd. Signature checke. File check3. 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. Proactive, Heuristic, and Real-time Scanning Engine (file and mail)6. Malicious Traffic Detection and Host Intrusion Prevention System7. Domain and IP Reputation Check8. Non-Intrusive Learning Pattern9. Cloud Security: Centralized definition updates thru cloud10. Scheduled and On-demand Scanning11. Configurable scanning priority (high, medium, and low)12. Configurable to set background scanning13. Customizable actions on malware of infected file (clean, quarantine, and delete)14. Ability to block attachments on Instant Messengers15. Website that capable to upload and analyze potential malware or virus16. Capable of scanning attached mobile devices	

B	WEB PROTECTION <ol style="list-style-type: none"> 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 7. Capable of implementing date wise restriction 	
C	MAIL ANTI-VIRUS & ANTI-SPAM PROTECTION <ol style="list-style-type: none"> 1. Incoming and outgoing emails scanning for spam and phishing emails with artificial intelligence and machine learning support. 2. Scanning must covered standard and SSL mail ports. 3. Support for the following filtering layers: <ul style="list-style-type: none"> • Customizable word/phrase filtering • Mail Non-Intrusive Learning Pattern • Email Header and X-Spam Rules Checking • SPF Checking • 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. 10. Capable of domain whitelisting for email attachment 	
D	DEVICE AND APPLICATION CONTROL <ol style="list-style-type: none"> 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. 	
E	PRIVACY PROTECTION AND MAINTENANCE <ol style="list-style-type: none"> 1. Integrated virtual keyboard for key logger evasion. 2. Ability to clear the following: <ul style="list-style-type: none"> • Temporary internet and windows temporary files • Remove temp files , cookies , MRU lists from registry • Browser history based on a schedule • Clear cache, cookies, plugins ActiveX, and history on a schedule. 	

F	RESCUE AND RECOVERY UTILITIES <ol style="list-style-type: none"> 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 	
G	RESCUE AND RECOVERY UTILITIES <ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> 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. 	
I	REPORTING <ol style="list-style-type: none"> 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 generate reports to *.html, *.xls, *.pdf. 5. Report Generation by weekly and monthly. 	

J	UNIFIED MANAGEMENT CONSOLE <ol style="list-style-type: none"> Centrally managed server via console and on heterogeneous platform (Windows, Linux, & MacOS) Real-time dashboard on the status of the endpoints (installed, updated, outdated and offline workstations) Report Generation of the following: <ul style="list-style-type: none"> Installed count Not Installed Count Updated non-updated Top 10 infected computers Asset Changes Policy deployment based on per user and per group Auto-grouping for managed workstations Remote application silent installation Configurable FTP and HTTP update source QoS configuration for workstations Role based administrative access One-time password facility for temporary administrator access with time duration settings. Outbreak notification thru email based on configurable threshold Integration with 3rd party CRM via SNMP Administrator broadcast messaging Active Directory/LDAP Synchronization Scheduled Task Deployment System Control for forced shutdown, forced restart and lock computer 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. 	
K	ASSET MANAGEMENT AND PATCH MANAGEMENT <ol style="list-style-type: none"> Integrated asset management <ul style="list-style-type: none"> Software and Hardware Inventory License Inventory Hardware changes Application Installed Workstation software/hardware modification alerts and reports. Ability generate reports to *.html, *.xls, *.pdf for the asset inventory. Capability to check critical patches installed on workstation and able to push critical updates on workstation. 	
L	GATEWAY ANTIVIRUS & ANTI-SPAM <ol style="list-style-type: none"> Scans, clean or quarantine all the email in real-time for Viruses, Worms, Trojans, Spyware, Adware and hidden malicious content. Greylisting - capable which mails from unknown senders are temporarily rejected, as most spamming servers do not try to send the same mails again if rejected for the first time. In case, the mail is legitimate, the originating server re-attempts to send the mail, which is then accepted. 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. Must have a heuristic driven dual anti-virus engine. With in-built technologies to filter out image spam. Capable of LDAP & POP3 Authentication 	
M	CERTIFICATIONS <ol style="list-style-type: none"> VB 100 Virus Definition AV Test ICSA Lab 	

N	OPERATING SYSTEMS SUPPORTED		
	1. Clients - Workstation Operating System 2. Windows: XP SP 2 / Vista / Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / 2000 (Workstation) [All 32-bit and 64-bit Editions] 3. Server- Server Class OS 4. Windows: 2019 / 2016 / 2012 / SBS 2011 / Essential / 2008 R2 / 2008 / 2003 / R2 / 2003 / 2000 [All 32-bit and 64-bit Editions] 5. 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] 6. 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)		
SUPPORT			
	1. The Bidder shall provide daily 8 by 5 phone, email, and remote support with critical level on site assistance 2. The Bidder must have access to high-level of support via the principal for critical level concerns 3. The Bidder must provide professional implementation services 4. The Bidder must provide an annual health check to ensure that the product is properlyworking 5. The Bidder must provide pro-active Threat Management - giving MARINA alerts should there be any malware threat detected in other parts of the world that may pose a problem for the MARINA.		
OTHERS			
	1. The winning bidder is required to conduct knowledge transfer for the solution delivered for at most 5 people. The total number of training days should not exceed 3. All costs related to the training will be shouldered by the winning bidder. These include but not limited to, lease of venue, meals, transportation of participants to and from the training venue, trainer fees, etc. MARINA may, at its discretion, prefertoconductthetraininginitsofficepremises.In that case, the lease of venue may be waived. The training must be conducted within 15 calendar days from implementation acceptance.		
	2. At the end of the implementation phase, the winning bidder must submit a comprehensive documentation on the final setup. The documentation should configuration settings and allmanuals.		
	QTY. 500 CORPORATE ANTIVIRUS LICENSE WITH HYBRID NETWORK SUPPORT (2YEARS SUBSCRIPTION)	UNIT COST	TOTAL COST

**The above quoted prices are inclusive of all costs and applicable taxes.*

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

SUPPLY, DELIVERY, INSTALLATION AND CONFIGURATION OF FIVE HUNDRED (500) CORPORATE ANTIVIRUS LICENSE WITH HYBRID NETWORK SUPPORT (2 YEAR SUBSCRIPTION)		
Code	Technical Specification	Delivery Date**
A	FILE ANTI-VIRUS & ANTI-MALWARE <ol style="list-style-type: none"> 1. Dedicated engine for Ransomware detection and blocking. 2. Ransomware protection must have the following checking process: <ol style="list-style-type: none"> a. Reserve check b. Behavioral check c. Resources check d. Signature check e. 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. Proactive, Heuristic, and Real-time Scanning Engine (file and mail) 6. Malicious Traffic Detection and Host Intrusion Prevention System 7. Domain and IP Reputation Check 8. Non-Intrusive Learning Pattern 9. Cloud Security: Centralized definition updates thru cloud 10. Scheduled and On-demand Scanning 11. Configurable scanning priority (high, medium, and low) 12. Configurable to set background scanning 13. Customizable actions on malware of infected file (clean, quarantine, and delete) 14. Ability to block attachments on Instant Messengers 15. Website that capable to upload and analyze potential malware or virus 16. Capable of scanning attached mobile devices 	The Winning bidder is required to deliver and deploy the solution within 30 calendar days after issuance of Notice to Proceed (NTP)
B	WEB PROTECTION <ol style="list-style-type: none"> 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 7. Capable of implementing date wise restriction 	

C	MAIL ANTI-VIRUS & ANTI-SPAM PROTECTION <ol style="list-style-type: none"> 1. Incoming and outgoing emails scanning for spam and phishing emails with artificial intelligence and machine learning support. 2. Scanning must covered standard and SSL mail ports. 3. Support for the following filtering layers: <ul style="list-style-type: none"> • Customizable word/phrase filtering • Mail Non-Intrusive Learning Pattern • Email Header and X-Spam Rules Checking • SPF Checking • 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. 10. Capable of domain whitelisting for email attachment 	The Winning bidder is required to deliver and deploy the solution within 30 calendar days after issuance of Notice to Proceed (NTP)
D	DEVICE AND APPLICATION CONTROL <ol style="list-style-type: none"> 8. Password protection for USB removable devices. 9. Password protection for the uninstallation of the endpoint security. 10. Capability to keep a copy of files copied from endpoint to external storage device and vice versa. 11. Configurable to allow or block CD/DVD Drives, Web Cam, External Storage and any USB devices. 12. USB Vaccination Tool for USB Storage Devices. 13. Application Control: Whitelisting and blacklisting of application which are only allowed by the administrator. 14. Time-based Application Restriction. 	
E	PRIVACY PROTECTION AND MAINTENANCE <ol style="list-style-type: none"> 1. Integrated virtual keyboard for key logger evasion. 2. Ability to clear the following: <ul style="list-style-type: none"> • Temporary internet and windows temporary files • Remove temp files , cookies , MRU lists from registry • Browser history based on a schedule • Clear cache, cookies, plugins ActiveX, and history on a schedule. 	
F	RESCUE AND RECOVERY UTILITIES <ol style="list-style-type: none"> 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 	

G	RESCUE AND RECOVERY UTILITIES <ol style="list-style-type: none"> 5. Rescue Disc: Rescue mode boot option so that scanning is possible without loading the installed OS 6. Rescue USB: Linux-based Rescue USB for cleaning of rootkits and file infectors 7. 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. 8. Backup tool with encryption functionality for additional security 	The Winning bidder is required to deliver and deploy the solution within 30 calendar days after issuance of Notice to Proceed (NTP)
H	USER DEFINED FILE AND FOLDER PROTECTION <ol style="list-style-type: none"> 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. 	
I	REPORTING <ol style="list-style-type: none"> 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 generate reports to *.html, *.xls, *.pdf. 5. Report Generation by weekly and monthly. 	
J	UNIFIED MANAGEMENT CONSOLE <ol style="list-style-type: none"> 1. Centrally managed server via console and on heterogeneous platform (Windows, Linux, & MacOS) 2. Real-time dashboard on the status of the endpoints (installed, updated, outdated and offline workstations) 3. Report Generation of the following: <ul style="list-style-type: none"> • Installed count • Not Installed Count • Updated non-updated • Top 10 infected computers • Asset Changes 4. Policy deployment based on per user and per group 5. Auto-grouping for managed workstations 6. Remote application silent installation 7. Configurable FTP and HTTP update source 8. QoS configuration for workstations 9. Role based administrative access 10. One-time password facility for temporary administrator access with time duration settings. 11. Outbreak notification thru email based on configurable threshold 12. Integration with 3rd party CRM via SNMP 13. Administrator broadcast messaging 14. Active Directory/LDAP Synchronization 15. Scheduled Task Deployment 16. System Control for forced shutdown, forced restart and lock computer 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. 	

K	ASSET MANAGEMENT AND PATCH MANAGEMENT <ol style="list-style-type: none"> 1. Integrated asset management <ul style="list-style-type: none"> • Software and Hardware Inventory • License Inventory • Hardware changes • Application Installed 2. Workstation software/hardware modification alerts and reports. 3. Ability 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. 	The Winning bidder is required to deliver and deploy the solution within 30 calendar days after issuance of Notice to Proceed (NTP)
L	GATEWAY ANTIVIRUS & ANTI-SPAM <ol style="list-style-type: none"> 1. Scans, clean or quarantine all the email in real-time for Viruses, Worms, Trojans, Spyware, Adware and hidden malicious content. 2. Greylisting - capable which mails from unknown senders are temporarily rejected, as most spamming servers do not try to send the same mails again if rejected for the first time. In case, the mail is legitimate, the originating server re-attempts to send the mail, which is then accepted. 3. 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. 4. Must have a heuristic driven dual anti-virus engine. 5. With in-built technologies to filter out image spam. 6. Capable of LDAP & POP3 Authentication 	
M	CERTIFICATIONS <ol style="list-style-type: none"> 1. VB 100 Virus Definition 2. AV Test 3. ICSA Lab 	
N	OPERATING SYSTEMS SUPPORTED <ol style="list-style-type: none"> 1. Clients - Workstation Operating System 2. Windows: XP SP 2 / Vista / Windows 7 / Windows 8 / Windows 8.1 / 3. Windows 10 / 2000 (Workstation) [All 32-bit and 64-bit Editions] 4. Server- Server Class OS 5. Windows: 2019 / 2016 / 2012 / SBS 2011 / Essential / 2008 R2 / 2008 / 2003 / R2 / 2003 / 2000 [All 32-bit and 64-bit Editions] 6. 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 / 7. Fedora 5.0 and above /Ubuntu 6.06 and above [All 32-bit and 64-bit Editions] 8. 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) 	

SUPPORT		
1.	The Bidder shall provide daily 8 by 5 phone, email, and remote support with critical level on site assistance	The Winning bidder is required to deliver and deploy the solution within 30 calendar days after issuance of Notice to Proceed (NTP)
2.	The Bidder must have access to high-level of support via the principal for critical level concerns	
3.	The Bidder must provide professional implementation services	
4.	The Bidder must provide an annual health check to ensure that the product is properly working	
5.	The Bidder must provide pro-active Threat Management - giving MARINA alerts should there be any malware threat detected in other parts of the world that may pose a problem for the MARINA.	
OTHERS		
1.	The winning bidder is required to conduct knowledge transfer for the solution delivered for at most 5 people. The total number of training days should not exceed 3. All costs related to the training will be shouldered by the winning bidder. These include but not limited to, lease of venue, meals, transportation of participants to and from the training venue, trainer fees, etc. MARINA may, at its discretion, prefer to conduct the training in its office premises. In that case, the lease of venue may be waived. The training must be conducted within 15 calendar days from implementation acceptance.	The Winning bidder is required to deliver and deploy the solution within 30 calendar days after issuance of Notice to Proceed (NTP)
2.	At the end of the implementation phase, the winning bidder must submit a comprehensive documentation on the final setup. The documentation should configuration settings and all manuals.	
QTY. <u>500</u> CORPORATE ANTIVIRUS LICENSE WITH HYBRID NETWORK SUPPORT (2YEARS SUBSCRIPTION)		

FINANCIAL OFFER:

Please quote your **best for** the item below. Please do not leave any blank items. Indicate “0” if item being offered is for free.

SUPPLY, DELIVERY, INSTALLATION AND CONFIGURATION OF FIVE HUNDRED (500) CORPORATE ANTIVIRUS LICENSE WITH HYBRID NETWORK SUPPORT (2 YEAR SUBSCRIPTION)	
Approved Budget for the Contract (ABC)	Total Offered Quotation
Five Hundred Thousand Pesos (Php500,000.00)	<p>In words: _____</p> <p>_____</p> <p>_____</p> <p>_____</p> <p>In figures: _____</p> <p>_____</p> <p>_____</p> <p>_____</p>

PAYMENT DETAILS:

<i>Banking Institution:</i> _____
<i>Account Number:</i> _____
<i>Account Name:</i> _____
<i>Branch:</i> _____

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/s, to be denominated in Philippine peso shall include all taxes, duties and/or levies payable.
4. Quotations exceeding the Approved Budget for the Contract shall be rejected.
5. 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.
6. 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.
7. The item/s shall be delivered according to the requirements specified in the Technical Specifications.
8. The MARINA shall have the right to inspect and/or to test the goods to confirm their conformity to the technical specifications.
9. 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.
10. **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 contractor's account.**
11. 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

SUPPLY, DELIVERY, INSTALLATION AND CONFIGURATION OF FIVE HUNDRED (500) CORPORATE ANTIVIRUS LICENSE WITH HYBRID NETWORK SUPPORT (2 YEARS 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 Five Hundred Thousand Pesos (500,000.00), inclusive of all applicable government charges.

II. 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:
 - a. Reserve check
 - b. Behavioral check
 - c. Resources check
 - d. Signature check
 - e. 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. Proactive, Heuristic, and Real-time Scanning Engine (file and mail)
6. Malicious Traffic Detection and Host Intrusion Prevention System
7. Domain and IP Reputation Check
8. Non-Intrusive Learning Pattern
9. Cloud Security: Centralized definition updates thru cloud
10. Scheduled and On-demand Scanning
11. Configurable scanning priority (high, medium, and low)
12. Configurable to set background scanning
13. Customizable actions on malware of infected file (clean, quarantine, and delete)
14. Ability to block attachments on Instant Messengers
15. Website that capable to upload and analyze potential malware or virus
16. Capable of scanning attached mobile devices

B. 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
7. Capable of implementing date wise restriction

C. 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 covered standard and SSL mail ports.
3. Support for the following filtering layers:
 - Customizable word/phrase filtering
 - Mail Non-Intrusive Learning Pattern
 - Email Header and X-Spam Rules Checking
 - SPF Checking
 - 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.
10. Capable of domain whitelisting for email attachment

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:
 - Temporary internet and windows temporary files
 - Remove temp files , cookies , MRU lists from registry
 - Browser history based on a schedule
 - 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

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.

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 generate reports to *.html, *.xls, *.pdf.
5. Report Generation by weekly and monthly.

J. Unified Management Console

1. Centrally managed server via console and on heterogeneous platform (Windows, Linux, & MacOS)
2. Real-time dashboard on the status of the endpoints (installed, updated, outdated and offline workstations)
3. Report Generation of the following:
 - Installed count
 - Not Installed Count
 - Updated non-updated
 - Top 10 infected computers

- Asset Changes
- 4. Policy deployment based on per user and per group
- 5. Auto-grouping for managed workstations
- 6. Remote application silent installation
- 7. Configurable FTP and HTTP update source
- 8. QoS configuration for workstations
- 9. Role based administrative access
- 10. One-time password facility for temporary administrator access with time duration settings.
- 11. Outbreak notification thru email based on configurable threshold
- 12. Integration with 3rd party CRM via SNMP
- 13. Administrator broadcast messaging
- 14. Active Directory/LDAP Synchronization
- 15. Scheduled Task Deployment
- 16. System Control for forced shutdown, forced restart and lock computer 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.

K. Asset Management and Patch Management

1. Integrated asset management
 - Software and Hardware Inventory
 - License Inventory
 - Hardware changes
 - Application Installed
2. Workstation software/hardware modification alerts and reports.
3. Ability 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.

L. Gateway Antivirus & Anti-Spam

1. Scans, clean or quarantine all the email in real-time for Viruses, Worms, Trojans, Spyware, Adware and hidden malicious content.
2. Greylisting - capable which mails from unknown senders are temporarily rejected, as most spamming servers do not try to send the same mails again if rejected for the first time. In case, the mail is legitimate, the originating server re-attempts to send the mail, which is then accepted.
3. 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.
4. Must have a heuristic driven dual anti-virus engine.
5. With in-built technologies to filter out image spam.
6. Capable of LDAP & POP3 Authentication

M. Certifications

1. VB 100 Virus Definition
2. AV Test
3. ICSA Lab

N. Operating Systems Supported

1. **Clients - Workstation Operating System**
2. **Windows:** XP SP 2 / Vista / Windows 7 / Windows 8 / Windows 8.1 /
3. Windows 10 / 2000 (Workstation) [All 32-bit and 64-bit Editions]
4. **Server- Server Class OS**
5. **Windows:** 2019 / 2016 / 2012 / SBS 2011 / Essential / 2008 R2 / 2008 / 2003 / R2 / 2003 / 2000 [All 32-bit and 64-bit Editions]
6. **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 /
7. Fedora 5.0 and above /Ubuntu 6.06 and above [All 32-bit and 64-bit Editions]
8. **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)

III. Support

1. The Bidder shall provide daily 8 by 5 phone, email, and remote support with critical level onsite assistance
2. The Bidder must have access to high-level of support via the principal for critical level concerns
3. The Bidder must provide professional implementation services
4. The Bidder must provide an annual health check to ensure that the product is properly working
5. The Bidder must provide pro-active Threat Management - giving MARINA alerts should there be any malware threat detected in other parts of the world that may pose a problem for the MARINA.

IV. Others

1. The winning bidder is required to conduct knowledge transfer for the solution delivered for at most 5 people. The total number of training days should not exceed 3. All costs related to the training will be shouldered by the winning bidder. These include but not limited to, lease of venue, meals, transportation of participants to and from the training venue, trainer fees, etc. MARINA may, at its discretion, prefer to conduct the training in its office premises. In that case, the lease of venue may be waived. The training must be conducted within 15 calendar days from implementation acceptance.

2. At the end of the implementation phase, the winning bidder must submit a comprehensive documentation on the final setup. The documentation should configuration settings and all manuals.

IV. Delivery

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

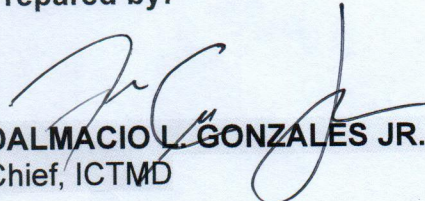
V. Qualification of the Supplier

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

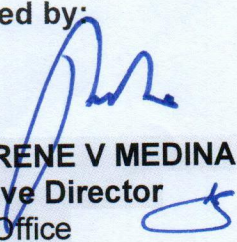
VI. Payment

- 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

Approved by:


VADM RENE V MEDINA AFP (Ret)
Executive Director
STCW Office



REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF TRANSPORTATION

MARITIME INDUSTRY AUTHORITY



PURCHASE REQUEST

Office: STCW OFFICE

PR No. :

2021-07-304

Division/Section: ICTMD

SAI No. :

30 JULY 2021

Date Request: July 14, 2021

Item No.	Unit	Item Description	Quantity	Unit Cost	Total Cost
		Supply, Delivery, Installation and Configuration of Five Hundred (500) Corporate Antivirus License With Hybrid Network Support (2 Years Subscription)			500,000.00
*****	*****	*****	*****	*****	*****

Requisitioning Officer

Signature:

Printed Name:

VADM RENE V MEDINA AFP (Ret)

Designation

Executive Director
STCW Office

Purpose:

To prevent, scan, detect and delete viruses from computers being used by MARINA Offices.

CERTIFICATION



FUNDS AVAILABLE

NO FUNDS AVAILABLE

RALPH A. NARVAEZ

Chief, Budget Division

☐ Approved

☐ Disapproved

PR Approver

Signature:

Printed Name:

VADM ROBERT A EMPEDRAD AFP (Ret)

Designation

Administrator

Note: