www.marina.gov.ph

TERMS OF REFERENCE

FOR

THE SUPPLY, DELIVERY, INSTALLATION AND CONFIGURATION OF THREE HUNDRED UNITS OF CORPORATE ANTIVIRUS LICENSE WITH HYBRID NETWORK SUPPORT (2 YEARS SUBSCRIPTION)

BACKGROUND

The Maritime Industry Authority (MARINA) was created on 01 June 1974 as an attached Agency to the Office of the President (OP) with the issuance of Presidential Decree No. 474, otherwise known as the Maritime Industry Decree of 1974, to integrate the development, promotion and regulation of the maritime industry in the country. With the creation of the Ministry (now Department) of Transportation (DOTr) by virtue of Executive Order No. 546, the MARINA was attached to the DOTr for policy and program coordination on 23 July 1979. By virtue of Republic Act No. 10635, the Maritime Industry Authority (MARINA) is established as the "Single Maritime Administration" responsible for the implementation and enforcement of the 1978 International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, as amended, and International Agreements or Covenants related thereto.

OBJECTIVE

Ensure that the workstations being used at Marina is protected from Viruses, Spyware, Identity Theft and Spam (Uninterrupted service)

RATIONALE

Revised implementing rules and regulations of republic act no. 9184, otherwise known as the government procurement reform act.

Section 46. Lease Contracts

The lease of construction and office equipment, including computers, communication and information technology equipment, are subject to the same public bidding and to the processes prescribed under the Act and this IRR. Lease may also cover lease purchases or lease-to-own and similar variations.

TECHNICAL SPECIFICATIONS

Technical Specifications:	Details
Operating Systems Supported	• Clients - Workstation Operating System > Windows 7/ Vista / XP / 2000 (Workstation) [All 32-bit and 64-bit Editions] • Server– Server Class OS > Windows 2000 / 2003 & Windows 2008 [All 32-bit and 64-bit Editions]
Anti-virus	• Product should have unique patented scanning and detection technology for Malwares and dedicated engine for **Ransomware** detection and blocking • Proactive Scanner with AI and Machine Learning within the scan engine • Product should have MWL technology for real time protection and winsock layer filtering • Product should have intelligent self-protection • Product should have real-time Email Scanner at endpoint • Should be able to protect against Keylogger , File-less Malware , Rootkits, Sypware, Ransomwares and Zero-day attacks and should be EDR compliant. • Product should have real-time file monitor with EDR capabilities. • Product should have a on demand scanner • Product should have Malware mitigation of URLs capabilities with cloud intelligence • Product should have capabilities to do fast scanning with technologies based on time saving logics during scans
Mail Anti-Virus	• Product should scan in-coming/Out-Going emails at the client • Product should be able to block attachments based on type • Product should be able to archive emails and attachments • Product should be able to take actions on malicious emails based on user defined actions • Product should be have customizable alert notifications for various events • Product should have a archival email viewer
Anti-spam	• Product should have a real-time anti-spam engine with based on Artificial Intelligence • Product should have a real-time anti Mail Phishing technology for clients • Product should have a customizable action for spam/phishing emails • Product should have Anti-SPAM engine with AI technology

Web Protection	• Product should be capable of controlling URL access based on categories and time basis • Product should have cloud intelligence capabilities for understanding and blocking malicious URLs • Product should have smart Anti-phishing filter based in intelligent heuristics • Product should be able to allow customizable policies as per user organizational security policies • Product should allow port access customizations for Url accesses. • Product should be EDR compliant based on log violations
Firewall Inbound and Outbound	• Product should include a two way state full intelligent firewall and EDR functionality • Product firewall should be able to deploy various rules based on IP Range, MAC Address , Trojan Rule, • Product firewall should automatically identify / whitelist internal DNS, DHCP data • Product firewall should be able to mitigate DDOS attacks • Product firewall should be able to mitigate Brute force attacks via RDP • Product firewall should be able to provide a network monitoring • Product firewall should be able provide all the events in real time and reports of violations
Anti-Phishing	Product should include Anti-phishing technology
Rescue Mode	Should have a rescue mode boot option so that scanning is possible without loading the installed OS
Cloud Security Network	Product should have a cloud security network support
Secure Delete	Product should have the 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.
Backup and Restore	Product should have a backup tool with encryption functionality for additional security
Password Protection	Product should be password protected on clients
Asset & System Inventory Management	Product should capable for system administrators to remotely query about the hardware and software specification of the workstation deployed in the network.

Embedded Remote Support Application	• Product should be integrated with remote support client so that OEM can provide quick support • Product should receive remote technical support from the country distributor and the developer internationally available and online security connection via embedded remote support tool
Virtual Keyboard	Product should be integrated with a data generating input tool which should not be susceptible to key loggers
User Defined File and Folder Protection	Product should have a DL function which data can be marked for protection against access and modification over network
Endpoint Security Device Control	• Product should have password protection for USB devices • Product should be able to block USB Autoplay • Product should be able to keep a copy of files copied from Endpoint to external device and vice versa. • Product should be able to block CD/DVD Drives • Product should be able to block Web Cams • Product should be able to block SD cards • Product should provide a facility of read only mode of USB Storage devices • Product should have complete Application control module with Whitelisting/Blacklisting based on time restrictions • Product should have USB Vaccination tools. So that the pen drive doesn't get infected if inserted in a infected machine. • Product should be able to block attachments
Privacy Protection	• Product should be able to erase temporary internet and windows temporary files • Product should be able to remove temp files , cookies , MRU lists from registry • Product should be able to clear browser history based on a schedule • Product should be able to clear cache , cookies , plugins Activex , history on a schedule. • Product should have a secure delete function
Unified Management Console	• Product should be able to manage all the functionality from a centrally managed server via console and on heterogeneous platform (Windows , Linux, Mac)

	• Product should be able to provide a real time dashboard on the status of the Endpoints • Product should be able to provide a real time dashboard on the security status of all the endpoints • Product should be able to provide various reports (Installed count , Not Installed Count , Updated / Non Updated etc) • Product should be able to deploy policies from the primary centralized server • Product should be able to provide group based categorization for viewing, policy deployment , task schedule and for complete MIS • Product should provide OTP facility for temporary access which should be time based • Product should have a Outbreak Prevention task in case of a virus attack • Product should have a asset management (Software/hardware) module with asset change alerts and reports • Product should have hierarchal administrative role based user creation • Product should be configurable over http and FTP updates to the client • Product should be able to integrate with 3rd party CRM via SNMP and have EDR capabilities with 3rd party apps like syslog server and splunk forwarders • Product should be able to do bandwidth management with QOS and able to define sizes of the updates • Product should be able to provide auto groupings for endpoints functionality which can be integrated into customized setups
Tools	• Product should be able to create a bootable USB with integrated AV toolkit • Product should be able to restore default settings • Product should have integrated interface to upload virus samples • Product should have a vaccination tool for USB or external HDDS to block infections • Product should be able to download Windows Essential updates • Product should have a registry cleaner inbuilt
Technical Support	FREE Installation and Technical Training FREE Engine Update and Upgrade 24 / 7 International Helpdesk Support (Phone, Chat, and E-mail) 8 / 5 Onsite Technical Support

	8 / 5 Remote technical assistance (Phone, Chat, and E-mail)
Certifications	• VB 100 Virus Definition • ICSA Labs Anti-Virus
Others	• Solution provided must be compatible with the existing anti-virus used (this is imperative to achieve standardized and streamlined deployment and managed of security solutions).

TRANSFER OF TECHNOLOGY

- The bidder must provide a comprehensive training program to all of the marina-STCW endorsed staff Installing, Configuring, Administering and Configuring the Anti-Virus Solution.

- The training must be detailed enough for the technical participants to be able to completely operate and maintain the whole system. The training must also include trouble shooting, preventive maintenance, etc.

- Appropriate training manuals must be provided for each participant. Training manuals must be easy to understand and comprehend.

- Training and Technology Transfer should be conducted before final project acceptance.

- All expenses incurred during the training such as training venue, equipment required for the training and food shall be shouldered by the winning bidder.

QUALIFICATION OF THE SUPPLIER

The supplier must be legally registered, has at least 5 years experience in supplying computers and software and should submit copies of Client Satisfactory Certificates from at least two (2) clients for the last two (2) years.

RESPONSIBILITY OF THE SUPPLIER

- Deliver and install all components and software within fifteen (15) days upon receipt of Notice to Proceed (NTP);
- Maximum of one (1) day response time from time reported.
- Provide 8X5 call and onsite technical support with two (2) hours response time for technical problem that requires on-site services. For problem reported after 4:00 PM, services shall be rendered in the morning of the following business day;
- Provide documentation of all components and peripherals.

RESPONSIBILITY OF THE MARINA

- Supervise the delivery, installation and configuration all components and software;
- Install other software not covered by the supplier; and
- Issue Inspection and Acceptance Report to the supplier as basis of payment.

WARRANTY

- Warranty shall be 2 years.

APPROVED BUDGET FOR THE CONTRACT

The Approved Budget for the Contract (ABC) for the project is Five Hundred Thousand Pesos (₱500,000.00), inclusive of all applicable government taxes and charges.