TERMS OF REFERENCE

PROCUREMENT OF VARIOUS INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) EQUIPMENT FOR THE MARITIME INDUSTRY AUTHORITY (MARINA)

A. Background

The Maritime Industry Authority (MARINA) is a government agency established pursuant to Presidential Decree No. 474 and attached to the Department of Transportation (DOTr). In compliance with the Republic Act No. 9184 known as the "Government Procurement Reform Act", MARINA will be procuring ICT equipment for the official use in the MARINA Central Office and MARINA Regional Offices.

B. Objective

To procure various branded and new ICT equipment that can assist MARINA employees in increasing the efficiency and speed of the process and other official use in the MARINA Central Office and MARINA Regional Offices.

C. Approved Budget for the Contract (ABC)

The Approved Budget for the Contract (ABC) is One Hundred Thirty Four Million Pesos **(Php 134,000,000.00)**, inclusive of VAT and other applicable government taxes to be charged against the National Expenditure Program FY 2024 .

D. Mode of Procurement

Bidding will be conducted through open competitive bidding procedures using a non-discretionary "pass/fail" criterion as specified in the 2016 revised Implementing Rules and Regulations (IRR) of Republic Act (RA) No. 9184.

E. Eligibility Requirements

1) Class "A" Documents

Legal Documents

1.1 Registration certificate from SEC, Department of Trade and Industry (DTI) for sole proprietorship, or CDA for cooperatives.

1.2 Mayor's/Business permit issued by the city or municipality where the principal place of business of the prospective bidder is located, or the

equivalent document for Exclusive Economic Zones or Areas. A recently expired Mayor's/Business permit together with the official receipt as proof that the prospective bidder has applied for renewal within the period prescribed by the concerned local government unit, shall be accepted by the PhilGEPS for the purpose of updating the PhilGEPS Certificate of Registration and Membership in accordance with Section 8.5.2 of the 2016 Revised IRR of RA 9184.

1.3 Tax clearance per E.O. 398, s. 2005, as finally reviewed and approved by the Bureau of Internal Revenue (BIR). Technical Documents

Technical Documents

1.4 Statement of the bidder of all its ongoing government and private contracts, including contracts awarded but not yet started, if any, whether similar or not similar in nature and complexity to the contract to be bid.

1.5 Statement of the bidder's Single Largest Completed Contract (SLCC) similar to the contract to be bid, except under conditions provided for in Sections 23.4.1.3 and 23.4.2.4 of the 2016 Revised IRR of RA 9184, within the relevant period as provided in the Bidding Documents in the case of Goods.

(For this purpose, contracts similar to the Project shall be:
a. Supply and delivery of ICT Equipment
b. Completed within Three (3) years prior to the deadline for the submission and receipt of bids)

Financial Documents

1.6 The bidder's audited financial statements, showing, among others, the bidder's total and current assets and liabilities, stamped "received" by the BIR or its duly accredited and authorized institutions, for the preceding calendar year which should not be earlier than two (2) years from the date of bid submission

1.7 The bidder's computation of Net Financial Contracting Capacity (NFCC). However, in the case of procurement of Goods, a bidder may submit a committed Line of Credit from a Universal or Commercial Bank, in lieu of its NFCC computation.

In lieu of the Class "A" eligibility documents mentioned under Section 8.5.2 of the 2016 Revised IRR of RA 9184, the Bidder shall only submit a valid and updated PhilGEPS Certificate of Registration and Membership in accordance with Section 8.5.2 of this IRR for purposes of determining eligibility

2.Class "B" Document

For Goods, valid joint venture agreement (JVA), in case the joint venture is already in existence. In the absence of a JVA, duly notarized statements from all the potential joint venture partners should be included in the bid, stating that they will enter into and abide by the provisions of the JVA in the event

that the bid is successful. Failure to enter into a joint venture in the event of a contract award shall be ground for the forfeiture of the bid security.

Each partner of the joint venture shall submit their respective PhilGEPS Certificates of Registration in accordance with Section 8.5.2 of the 2016 Revised IRR of RA 9184. The submission of technical and financial eligibility documents by any of the joint venture partners constitutes compliance: Provided, That the partner responsible to submit the NFCC shall likewise submit the Statement of all of its ongoing contracts and Audited Financial Statements.

F. MARINA Requirements

In addition to the mandated requirements under RA 9184 and its IRR, the bidders must comply with the MARINA requirements, as follows:

1. Bidders must be in the ICT business for at least ten (10) years.
2. The brand of the servers, desktops, and laptops must be Energy Star compliant.
3. The supplier must be an authorized reseller of the servers, desktop, and laptop brands being offered and must submit a certification from the manufacturer. *(to be submitted as part of the bid)*
4. Bidders must have regional presence for desktop and laptop *(items 1 to 5 of the deliverables)* and must submit a list of their Authorized Repair Service Centers in all regions with the address and name of the contact person. *(to be submitted as part of the bid)*.
    - MRO I and II – La Union
    - MRO IV – Batangas
    - MRO V – Legaspi
    - MRO VI- Iloilo
    - MRO VII- Cebu
    - MRO VIII- Tacloban
    - MRO IX- Zamboanga
    - MRO X- Cagayan de Oro
    - MRO XI- Davao
    - MRO XII- General Santos
    - MRO XIII-Butuan
    - Where there is none in a region, indicate the nearest Service Center in the adjoining region
5. The memorandum of agreement, contract, or memorandum of understanding of the bidder and their authorized repair/service center in all regions must be submitted as part of the bid.
6. The bidder must provide a certificate from the manufacturer that the Operating System installed is Genuine OS

G. Deliverables and Technical Specifications

Item	Unit	Description	Quantity
1	pcs.	All-in-One Desktop	31
2	pcs	Desktop	750
3	pcs	High-end Desktop for Production (Video and Graphics Design)	5
4	pcs.	Laptop	62
5	pcs.	Laptop for Production (Video and Graphics Design)	3
6	pcs.	Laptop (For Division Chiefs and Directors)	66
7	pcs	Laptop (For Programmers)	10
8	pcs	Tablet (For Engineers)	60
9	pcs	Tablet (For Top-Level Executives)	5
10	pcs.	Server	8
11	Package	Hyper Converged Infrastructure Solution	1
12	pc	Firewall Security Appliance	1

Below are the minimum specifications of the Thirty-One (31)   All-In-One Desktop to be procured:
- Processor : Core i7 13700 2.4 GHz, 14C 20T
- Memory: 16 GB DDR5 5200 SODIMM
- Graphics: Integrated Graphics
- Storage: 1 TB SSD M.2 2280 PCIe Gen4 TLC Opal
- Display Type: must be a 23.8" FHD, Anti-Glare,250 Nits
- Integrated Ethernet
- 5M Camera BK
- Dual Microphone
- 2x3 Internal Speaker
- Monitor Stand BK
- HDMI port
- Ports:
  1 USB-C 2.0 (supports data transfer, Power Delivery 3.0)
  1 USB 2.0

2 USB-C 3.2 Gen 2
1 USB 3.2 Gen 2(Supports Smart Power-On)
1 HDMI-in 1.4
1 HDMI-out 2.1 TMDS
1 headphone/microphone combo Jack

- USB Keyboard Black
- USB Mouse Black
- Intel Wi-Fi 6 AX201 2x2 AX & Bluetooth 5.1
- Must have recovery capability in a separate partition
- Must provide recovery CD/DVD (Operating System, Drivers, and other necessary recovery installers used)
- Must have F11 key or equivalent access to System Recovery
- Components (CPU, Keyboard, Mouse, Monitor) should be of the same brand
- Format hard disk in the manner of 40% for the system disk and 60% data disk
- With 650VA UPS
- With installed Licensed MS Office Home and Business Edition 2021
- With installed Licensed Microsoft Windows 11 Po 64
- With installed Licensed Anti-virus (3 years subscription, must be compatible with MARINA's existing Anti-virus)
  - Operating Systems Supported : (Windows: XP SP 2 / Vista / Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / 2000 (Workstation) [All 32-bit and 64-bit Editions]) (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]) (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 Yosemit (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)
  - Dedicated engine for Ransomware detection and blocking.
  - Ransomware protection must have the following checking process:
    - Reserve check
    - Behavioral check
    - Resources check
    - Signature check
    - File check
  - Patented scanning and detection technology for virus and malwares.
  - Protection for Windows at the WinSock layer, scanning thru WinSock Layer scan before it reaches to the operating system.
  - Proactive, Heuristic, and Real-time Scanning Engine (file and mail)
  - Malicious Traffic Detection and Host Intrusion Prevention System

- Domain and IP Reputation Check
- Non-Intrusive Learning Pattern
- Cloud Security: Centralized definition updates thru cloud
- Scheduled and On-demand Scanning
- Configurable scanning priority (high, medium, and low)
- Configurable to set background scanning
- Customizable actions on malware of infected file (clean, quarantine, and delete)
- Ability to block attachments on Instant Messengers
- Website that capable to upload and analyze potential malware or virus
- Mail Anti-Virus & Anti-Spam Protection
- Mail Gateway Anti-Spam and Content Security
- Capable to allow and block URL or website access based on database of pre-defined category or end-user customized category
- Allow and block URL or website access based on scheduled time
- Product should be able to allow customized web security policies in per user and per group
- Easy configuration for block all sites with allowed particular websites only
- Anti-phishing filter for websites based in intelligent heuristics
- Product should have cloud intelligence capabilities for understanding and blocking malicious URLs
- Device and Application Control
- Privacy Protection and Maintenance
- Rescue and Recovery Utilities
- User Defined File and Folder Protection (Network Protection)
- Unified Management Console
- Reporting
- Asset Management and Patch Management
- Certifications: VB 100 Virus Definition, AV Test, AV Comparatives
- Warranty: Three (3) years on parts and service (For the duration of the warranty period, the call-back response time (which may be through email, phone, or online support) shall be guaranteed within two (2) hours upon notification.
- On-site support shall be provided for the delivered items deployed in the Marina Central Office within the next business day from verbal or written notification.
- Provision of Service Units: Units that cannot be repaired within five (5) days shall be immediately replaced with a service unit of similar or higher specifications.

Below are the minimum specifications of the Seven Hundred Fifty (750) Desktop to be procured:

- Processor : Core i7 13700 (2.1 GHz, 16C 24 Threads
- Memory: 16 GB DDR4 3200 UDIMM
- Graphics: Integrated Graphics
- Storage: One (1) 1TB 2280 M.2 PCIe 4x4 NVMe TLC SSD
- Display Type: must be a 23.8" FHD, Anti-Glare, 250 Nits
- Integrated Gigabit Ethernet
- Integrated Intel AX211 Wi-Fi 6E 160 MHz +Bluetooth 5.3 WW WLAN
- Integrated Speaker
- Ports (Front):
  - 1 headphone/microphone combo;
  - 1 SuperSpeed USB Type-C® 10Gbps signaling rate;
  - 3 SuperSpeed USB Type-A 10Gbps signaling rate ;
- Ports (Rear):
  - 1 audio-out; 1 power connector;
  - 1 RJ-45; 1 HDMI 1.4;
  - 3 SuperSpeed USB Type-A 5Gbps signaling rate;
  - 1 DisplayPort™ 1.4;
  - 2 USB Type-A 480Mbps signaling rate
- USB Keyboard Black
- USB OPTICAL Mouse Black
- Must be 180 W internal power supply, up to 90% efficiency, active PFC; 240 W internal power supply, up to 92% efficiency, active PFC
- Security Features:
  - TPM 2.0 Embedded Security Chip
  - Can protect your PC with browser-based threat containment, AI-based malware   scanning, anti-phishing credential protection. No more than 5% of CPU utilization with application and services present and protects against never-before-seen attacks.
  - Can offer remote management tools that has an innovative way to empower remote administrator and local present administrator to remotely manage PC bios settings to serve the user quickly and securely.
  - Must have an ecosystem of protection to help defend the PC, including automated protections, customizable safeguards, and easy manageability that guards against PC attacks without interrupting employee productivity.
  - must have a BIOS-level feature that protects data by permanently destroying sensitive information from hard drives and solid-state drives, ensuring the deleted information can never be recovered or compromised.
- Must have recovery capability in a separate partition
- Must provide recovery CD/DVD (Operating System, Drivers, and other necessary recovery installers used)
- Must have F11 key or equivalent access to System Recovery

- Components (CPU, Keyboard, Mouse, Monitor) should be of the same brand
- Format hard disk in the manner of 40% for the system disk and 60% data disk
- With 650VA UPS
- With installed Licensed MS Office Home and Business Edition 2021
- With installed Licensed Microsoft Windows 11 Po 64
- With installed Licensed Anti-virus (3 years subscription, must be compatible with MARINA's existing Anti-virus)
  - Operating Systems Supported : (Windows: XP SP 2 / Vista / Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / 2000 (Workstation) [All 32-bit and 64-bit Editions]) (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]) (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 Yosemit (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)
  - Dedicated engine for Ransomware detection and blocking.
  - Ransomware protection must have the following checking process:
    - Reserve check
    - Behavioral check
    - Resources check
    - Signature check
    - File check
  - Patented scanning and detection technology for virus and malwares.
  - Protection for Windows at the WinSock layer, scanning thru WinSock Layer scan before it reaches to the operating system.
  - Proactive, Heuristic, and Real-time Scanning Engine (file and mail)
  - Malicious Traffic Detection and Host Intrusion Prevention System
  - Domain and IP Reputation Check
  - Non-Intrusive Learning Pattern
  - Cloud Security: Centralized definition updates thru cloud
  - Scheduled and On-demand Scanning
  - Configurable scanning priority (high, medium, and low)
  - Configurable to set background scanning
  - Customizable actions on malware of infected file (clean, quarantine, and delete)
  - Ability to block attachments on Instant Messengers
  - Website that capable to upload and analyze potential malware or virus

8

- Incoming and outgoing emails scanning for spam and phishing emails with artificial intelligence and machine learning support.
- Scanning must covered standard and SSL mail ports.
- 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
- Blocking of attachments based on type (pre-defined and customizable with wildcard support)
- Archival of Mail and Attachments with archived mail viewer.
- Product should be able to take actions on malicious emails based on user defined actions.
- Customizable alert notifications for various level of events in like of virus outbreak and data theft.
- Customizable actions for spam/phishing emails.
- Able to tag spam mails in subject line with SPAM for considered spam mails.
- Mail Gateway Anti-Spam and Content Security
- Capable to allow and block URL or website access based on database of pre-defined category or end-user customized category
- Allow and block URL or website access based on scheduled time
- Product should be able to allow customized web security policies in per user and per group
- Easy configuration for block all sites with allowed particular websites only
- Anti-phishing filter for websites based in intelligent heuristics
- Product should have cloud intelligence capabilities for understanding and blocking malicious URLs
- Device and Application Control
- Privacy Protection and Maintenance
- Rescue and Recovery Utilities
- User Defined File and Folder Protection (Network Protection)
- Unified Management Console
- Reporting
- Asset Management and Patch Management
- Certifications: VB 100 Virus Definition, AV Test, AV Comparatives

- Warranty: Three (3) years on parts and service (For the duration of the warranty period, the call-back response time (which may be through email, phone, or online support) shall be guaranteed within two (2) hours upon notification.
- On-site support shall be provided for the delivered items deployed in the Marina Central Office within the next business day from verbal or written notification.
- Provision of Service Units: Units that cannot be repaired within five (5) days shall be immediately replaced with a service unit of similar or higher specifications.

Below are the minimum specifications of the Five (5) High-end Desktop for Production (Video and Graphics Design) to be procured:

- Processor : 13th Gen Intel Core i9 13900 vPro (E-cores up to 4.20 GHz P-cores up to 5.20 GHz)
- Memory: Two (2) 16 GB DDR5 4000MHz SODIMM
- Graphics: NVIDIA RTX A2000 12GB GDDR6
- Storage: One (1) 1 TB SSD M.2 2280 PCIe Gen4 TLC Opal
  One (1) 256 GB SSD M.2 2280 PCIe Gen4 TLC Opal
- Display Type: must be a 23.8" FHD, Anti-Glare, 250 Nits
- Integrated Ethernet
- Single Speaker
- Ports
  5x USB 3.2 Gen 2
  2x Thunderbolt 4
  3x Display port 1.2
  1x Ethernet (2.5GbE RJ-45)
  1x Ethernet (GbE RJ-45)
  1x headphone/microphone combo jack
  Power Supply 230W
- USB Keyboard Black
- USB Mouse Black
- Intel Wi-Fi 6 AX201 2x2 AX & Bluetooth 5.1
- Feature:Self-Healing BIOS
- Must have recovery capability in a separate partition
- Must provide recovery CD/DVD (Operating System, Drivers, and other necessary recovery installers used)
- Must have F11 key or equivalent access to System Recovery
- Components (CPU, Keyboard, Mouse, Monitor) should be of the same brand
- Format hard disk in the manner of 40% for the system disk and 60% data disk
- With 650VA UPS
- With installed Licensed MS Office Home and Business Edition 2021
- With installed Licensed Microsoft Windows 11 Po 64
- With installed Licensed Anti-virus (3 years subscription, must be compatible with MARINA's existing Anti-virus)
  - Operating Systems Supported : (Windows: XP SP 2 / Vista / Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / 2000 (Workstation) [All 32-bit and 64-bit Editions])   (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]) (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 Yosemit (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)
  - Dedicated engine for Ransomware detection and blocking.

- Ransomware protection must have the following checking process:
  - Reserve check
  - Behavioral check
  - Resources check
  - Signature check
  - File check
- Patented scanning and detection technology for virus and malwares.
- Protection for Windows at the WinSock layer, scanning thru WinSock Layer scan before it reaches to the operating system.
- Proactive, Heuristic, and Real-time Scanning Engine (file and mail)
- Malicious Traffic Detection and Host Intrusion Prevention System
- Domain and IP Reputation Check
- Non-Intrusive Learning Pattern
- Cloud Security: Centralized definition updates thru cloud
- Scheduled and On-demand Scanning
- Configurable scanning priority (high, medium, and low)
- Configurable to set background scanning
- Customizable actions on malware of infected file (clean, quarantine, and delete)
- Ability to block attachments on Instant Messengers
- Website that capable to upload and analyze potential malware or virus
- Incoming and outgoing emails scanning for spam and phishing emails with artificial intelligence and machine learning support.
- Scanning must covered standard and SSL mail ports.
- 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
- Blocking of attachments based on type (pre-defined and customizable with wildcard support)
- Archival of Mail and Attachments with archived mail viewer.
- Product should be able to take actions on malicious emails based on user defined actions.
- Customizable alert notifications for various level of events in like of virus outbreak and data theft.
- Customizable actions for spam/phishing emails.
- Able to tag spam mails in subject line with SPAM for considered spam mails.
- Mail Gateway Anti-Spam and Content Security

- Capable to allow and block URL or website access based on database of pre-defined category or end-user customized category
- Allow and block URL or website access based on scheduled time
- Product should be able to allow customized web security policies in per user and per group
- Easy configuration for block all sites with allowed particular websites only
- Anti-phishing filter for websites based in intelligent heuristics
- Product should have cloud intelligence capabilities for understanding and blocking malicious URLs
- Device and Application Control
- Privacy Protection and Maintenance
- Rescue and Recovery Utilities
- User Defined File and Folder Protection (Network Protection)
- Unified Management Console
- Reporting
- Asset Management and Patch Management
- Certifications: VB 100 Virus Definition, AV Test, AV Comparative
- Warranty: Three (3) years on parts and service (For the duration of the warranty period, the call-back response time (which may be through email, phone, or online support) shall be guaranteed within two (2) hours upon notification.
- On-site support shall be provided for the delivered items deployed in the Marina Central Office within the next business day from verbal or written notification.
- Provision of Service Units: Units that cannot be repaired within five (5) days shall be immediately replaced with a service unit of similar or higher specifications.

Below are the minimum specifications of the Sixty Two (62) Laptop to be procured:
- Processor : 13th Gen Intel Core i7 1355U (E-cores up to 3.70 GHz P-cores up to 5.00 GHz)
- Memory: 16 GB DDR4 3200MHz (8GB Soldered + 8 GB SODIMM)
- Graphics: Integrated Intel Iris Xe Graphics
- Storage: One (1) 1 TB SSD M.2 2242 PCIe Gen4 TLC Opal
- 14"WUXGA (1920 x 1200), IPS, Anti-Glare, Non-Touch, 45%NTSc, 300 nits 60Hz, Narrow Bezel
- Ethernet port
- 720P HD RGB camera with microphone, with Privacy Shutter
- Speaker: 2x 2W Stereo Speaker(Internal)
- 1x USB-C 3.2 Gen 2 (supports data transfer, Power Delivery 3.0 and DisplayPort 1.4)
- 1x Thunderbolt 4/USB 4 40Gbps (support data transfer, Power Delivery 3.0 and Display Port 1.4)
- 1x USB 3.2 Gen 1 (Always On)
- 1x Ethernet (RJ-45)

- 1x HDMI 2.1, up to 4k/60Hz
- 1x headphone/microphone combo jack (3.5mm)
- Backlit, Black Painting
- Intel Wi-Fi 6 AX201 2x2 AX & Bluetooth 5.1
- With Fingerprint Reader
- 3 Cell Li- Polymer 47Wh
- 65W USB-C Low Cost 90% PCC 3pin AC Adapter
- Feature: Self-Healing BIOS
- Must have recovery capability in a separate partition
- Must provide recovery CD/DVD (Operating System, Drivers, and other necessary recovery installers used)
- Must have F11 key or equivalent access to System Recovery
- Format hard disk in the manner of 40% for the system disk and 60% data disk
- With installed Licensed MS Office Home and Business Edition 2021
- With installed Licensed Microsoft Windows 11 Po 64
- With installed Licensed Anti-virus (3 years subscription, must be compatible with MARINA's existing Anti-virus)
  - Operating Systems Supported : (Windows: XP SP 2 / Vista / Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / 2000 (Workstation) [All 32-bit and 64-bit Editions]) (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]) (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 Yosemit (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)
  - Dedicated engine for Ransomware detection and blocking.
  - Ransomware protection must have the following checking process:
    - Reserve check
    - Behavioral check
    - Resources check
    - Signature check
    - File check
  - Patented scanning and detection technology for virus and malwares.
  - Protection for Windows at the WinSock layer, scanning thru WinSock Layer scan before it reaches to the operating system.
  - Proactive, Heuristic, and Real-time Scanning Engine (file and mail)
  - Malicious Traffic Detection and Host Intrusion Prevention System
  - Domain and IP Reputation Check
  - Non-Intrusive Learning Pattern
  - Cloud Security: Centralized definition updates thru

cloud
- Scheduled and On-demand Scanning
- Configurable scanning priority (high, medium, and low)
- Configurable to set background scanning
- Customizable actions on malware of infected file (clean, quarantine, and delete)
- Ability to block attachments on Instant Messengers
- Website that capable to upload and analyze potential malware or virus
- Incoming and outgoing emails scanning for spam and phishing emails with artificial intelligence and machine learning support.
- Scanning must covered standard and SSL mail ports.
- 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
- Blocking of attachments based on type (pre-defined and customizable with wildcard support)
- Archival of Mail and Attachments with archived mail viewer.
- Product should be able to take actions on malicious emails based on user defined actions.
- Customizable alert notifications for various level of events in like of virus outbreak and data theft.
- Customizable actions for spam/phishing emails.
- Able to tag spam mails in subject line with SPAM for considered spam mails.
- Mail Gateway Anti-Spam and Content Security
- Capable to allow and block URL or website access based on database of pre-defined category or end-user customized category
- Allow and block URL or website access based on scheduled time
- Product should be able to allow customized web security policies in per user and per group
- Easy configuration for block all sites with allowed particular websites only
- Anti-phishing filter for websites based in intelligent heuristics
- Product should have cloud intelligence capabilities for understanding and blocking malicious URLs
- Device and Application Control
- Privacy Protection and Maintenance
- Rescue and Recovery Utilities
- User Defined File and Folder Protection (Network Protection)
- Unified Management Console
- Reporting
- Asset Management and Patch Management
- Certifications: VB 100 Virus Definition, AV Test, AV Comparatives

- Warranty: Three (3) years on parts and service, except for batteries, which are one (1) year. (For the duration of the warranty period, the call-back response time (which may be through email, phone, or online support) shall be guaranteed within two (2) hours upon notification.
- On-site support shall be provided for the delivered items deployed in the Marina Central Office within the next business day from verbal or written notification.
- Provision of Service Units: Units that cannot be repaired within five (5) days shall be immediately replaced with a service unit of similar or higher specifications.

Below are the minimum specifications of the Three (3) Laptop for Production (Video and Graphics Design)   to be procured:
- Processor : 13th Gen Intel Core i9 13950HX (E-cores up to 4.00 GHz P-cores up to 5.50 GHz)
- Memory: 32 GB DDR5 5600MHz (SODIMM) (2x16GB)
- Graphics: Integrated Intel UHD Graphics
- Storage: One (1) 1 TB SSD M.2 2280 PCIe Gen4 TLC Opal
- 16"WUXGA (1920 x 1200), IPS, Anti-Glare, Non-Touch, 100%RGB, 300 nits 60Hz, Low Blue Light
- Ethernet port
- 1080P FHD RGB camera with microphone, with Privacy Shutter
- Speaker: 2X 2W Stereo Speaker(Internal)
- 1x USB-C 3.2 Gen 2 (supports data transfer and Power Delivery 3.0)
- 2x Thunderbolt 4/USB 4 40Gbps (support data transfer, Power Delivery 3.0 and Display Port 1.4)
- 2x USB 3.2 Gen 1 (one Always On)
- 1x HDMI 2.1
- 1x Card reader
- 1x headphone/microphone combo jack (3.5mm)
- Backlit, Numeric Keypad
- Intel Wi-Fi 6E AX211 2x2 AX & Bluetooth 5.1
- With Fingerprint Reader
- 3 Cell Li- Polymer 94Wh
- 170W Slim 30% PCC 3pin AC Adapter
- Feature: Self-Healing Bios
- Must have recovery capability in a separate partition
- Must provide recovery CD/DVD (Operating System, Drivers, and other necessary recovery installers used)
- Must have F11 key or equivalent access to System Recovery
- Format hard disk in the manner of 40% for the system disk and 60% data disk
- With installed Licensed MS Office Home and Business Edition 2021
- With installed Licensed Microsoft Windows 11 Po 64
- With installed Licensed Anti-virus (3 years subscription, must be compatible with MARINA's existing Anti-virus)

- Operating Systems Supported : (Windows: XP SP 2 / Vista / Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / 2000 (Workstation) [All 32-bit and 64-bit Editions]) (Linux: RHEL 4 and above / CentOS 5.10 and above / SLES 10 SP3 and above / Debian 4.0 and above / open SuSe 10.1 and above Fedora 5.0 and above /Ubuntu 6.06 and above [All 32-bit and 64-bit Editions]) (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 Yosemit (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)
- Dedicated engine for Ransomware detection and blocking.
- Ransomware protection must have the following checking process:
  - o Reserve check
  - o Behavioral check
  - o Resources check
  - o Signature check
  - o File check
- Patented scanning and detection technology for virus and malwares.
- Protection for Windows at the WinSock layer, scanning thru WinSock Layer scan before it reaches to the operating system.
- Proactive, Heuristic, and Real-time Scanning Engine (file and mail)
- Malicious Traffic Detection and Host Intrusion Prevention System
- Domain and IP Reputation Check
- Non-Intrusive Learning Pattern
- Cloud Security: Centralized definition updates thru cloud
- Scheduled and On-demand Scanning
- Configurable scanning priority (high, medium, and low)
- Configurable to set background scanning
- Customizable actions on malware of infected file (clean, quarantine, and delete)
- Ability to block attachments on Instant Messengers
- Website that capable to upload and analyze potential malware or virus
- Incoming and outgoing emails scanning for spam and phishing emails with artificial intelligence and machine learning support.
- Scanning must covered standard and SSL mail ports.
- 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

- Blocking of attachments based on type (pre-defined and customizable with wildcard support)
- Archival of Mail and Attachments with archived mail viewer.
- Product should be able to take actions on malicious emails based on user defined actions.
- Customizable alert notifications for various level of events in like of virus outbreak and data theft.
- Customizable actions for spam/phishing emails.
- Able to tag spam mails in subject line with SPAM for considered spam mails.
- Mail Gateway Anti-Spam and Content Security
- Capable to allow and block URL or website access based on database of pre-defined category or end-user customized category
- Allow and block URL or website access based on scheduled time
- Product should be able to allow customized web security policies in per user and per group
- Easy configuration for block all sites with allowed particular websites only
- Anti-phishing filter for websites based in intelligent heuristics
- Product should have cloud intelligence capabilities for understanding and blocking malicious URLs
- Device and Application Control
- Privacy Protection and Maintenance
- Rescue and Recovery Utilities
- User Defined File and Folder Protection (Network Protection)
- Unified Management Console
- Reporting
- Asset Management and Patch Management
- Certifications: VB 100 Virus Definition, AV Test, AV Comparatives

- Warranty: Three (3) years on parts and service, except for batteries, which are one (1) year. (For the duration of the warranty period, the call-back response time (which may be through email, phone, or online support) shall be guaranteed within two (2) hours upon notification.
- On-site support shall be provided for the delivered items deployed in the Marina Central Office within the next business day from verbal or written notification.
- Provision of Service Units: Units that cannot be repaired within five (5) days shall be immediately replaced with a service unit of similar or higher specifications.

Below are the minimum specifications of the Sixty-six (66) Laptop (For Division Chiefs and Directors) to be procured:
- 8-Core CPU
- 7-Core GPU
- 8GB Unified Memory
- 256GB SSD Storage footnote
- 16-core Neural Engine

- 13-inch Retina display with True Tone
- Wireless
  - Wi-Fi
  - Wi-Fi 6 (802.11ax)
  - IEEE 802.11a/b/g/n/ac compatible
  - Bluetooth
  - Bluetooth 5.0 wireless technology
- Camera
  - 720p FaceTime HD camera
  - Advanced image signal processor with computational video
- Display Support
  - Simultaneously supports full native resolution on the built-in display at millions of colors and: One external display with up to 6K resolution at 60Hz
  - Thunderbolt 3 digital video output
  - Native DisplayPort output over USB-C
- Audio
  - Stereo speakers
  - Wide stereo sound
  - Support for Dolby Atmos playback
  - Three-mic array with directional beamforming
  - 3.5mm headphone jack
- Two Thunderbolt / USB 4 ports
- Magic Keyboard with Touch ID
- Force Touch trackpad
- 30W USB-C Power Adapter
- Licensed MS Office Home and Business Edition 2021 for Mac
- Warranty: One (1) year on parts and service On-Site for the Central Office, Carry-in for the Regional Offices

Below are the minimum specifications of the Ten (10) Laptop (For Programmers) to be procured:
- 10-core CPU
- 16-core GPU
- 16GB unified memory
- 14-inch Liquid Retina XDR display
- Apple M2 Pro chip or Apple M2 Max chip
- 1TB storage
- Liquid Retina XDR display
- 1080p FaceTime HD camera
- Up to 18 hours battery life
- Touch ID
- Apple M2 Pro chip
- Media engine
- Hardware-accelerated H.264, HEVC, ProRes, and ProRes RAW

- Video decode engine
- Video encode engine
- ProRes encode and decode engine
- SDXC card slot
- HDMI port
- MagSafe 3 port
- Wi-Fi
- Wi-Fi 6E (802.11ax)[5]
- Bluetooth
- Bluetooth 5.3
- High-fidelity six-speaker sound system with force-cancelling woofers
- Wide stereo sound
- Support for Spatial Audio when playing music or video with Dolby Atmos on built-in speakers
- Spatial Audio with dynamic head tracking when using AirPods (3rd generation), AirPods Pro, and AirPods Max
- Studio-quality three-mic array with high signal-to-noise ratio and directional beamforming
- 3.5mm headphone jack with advanced support for high-impedance headphones
- HDMI port supports multichannel audio output
- 67W USB-C Power Adapter
- Licensed MS Office Home and Business Edition 2021 for Mac
- Warranty: One (1) year on parts and service On-Site for the Central Office, Carry-in for the Regional Offices

Below are the minimum specifications of the Sixty (60) Tablet (For Engineers) to be procured:
- Wi-Fi + Cellular, 10th Generation
- Capacity : 256GB
- Display:
  - Liquid Retina display
  - 10.9-inch (diagonal) LED backlit Multi Touch display with IPS technology
  - 2360-by-1640-pixel resolution at 264 pixels per inch (ppi)
  - True Tone display
  - 500 nits brightness
  - Fingerprint-resistant oleo phobic coating
  - Supports Apple Pencil (1st generation)
- Chip
  - A14 Bionic chip
  - 6-core CPU
  - 4-core graphics
  - 16-core Neural Engine
- Camera
  - 12MP Wide camera, f/1.8 aperture

- Digital zoom up to 5x
- Five-element lens
- Autofocus with Focus Pixels
- Panorama (up to 63MP)
- Smart HDR 3
- Photo geotagging
- Auto image stabilization
- Burst mode
- Image formats captured: HEIF and JPEG
- Video Recording
  - 4K video recording at 24 fps, 25 fps, 30 fps, or 60 fps
  - 1080p HD video recording at 25 fps, 30 fps, or 60 fps
  - 720p HD video recording at 30 fps or 60 fps
  - Slo-mo video support for 1080p at 120 fps or 240 fps
  - Time-lapse video with stabilization
  - Extended dynamic range for video up to 30 fps
  - Video image stabilization
  - Cinematic video stabilization (1080p and 720p)
  - Continuous autofocus video
  - Playback zoom
  - Video formats captured: HEVC and H.264
- Cellular and Wireless
  - Wi-Fi 6 (802.11ax) with 2x2 MIMO; speeds up to 1.2 Gbps
  - Simultaneous dual band
  - Bluetooth 5.2
  - 5G NR (Bands n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n29, n30, n38, n40, n41, n48, n66, n71, n77, n78, n79)
  - FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 11, 12, 13, 14, 17, 18, 19, 20, 21, 25, 26, 28, 29, 30, 32, 66, 71)
  - TD-LTE (Bands 34, 38, 39, 40, 41, 42, 46, 48)
  - UMTS/HSPA/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)
  - Data only
  - Wi-Fi calling
  - eSIM
- Front Camera
  - Landscape 12MP Ultra Wide camera, 122° field of view
  - f/2.4 aperture
  - Smart HDR 3
  - 1080p HD video recording at 25 fps, 30 fps, or 60 fps
  - Time-lapse video with stabilization
  - Extended dynamic range for video up to 30 fps
  - Cinematic video stabilization (1080p and 720p)
  - Lens correction
  - Retina Flash
  - Auto image stabilization
  - Burst mode

- Video Calling
  - FaceTime video
  - Center Stage
  - iPad to any FaceTime-enabled device over Wi-Fi or cellular
- Audio Calling
  - FaceTime audio
  - iPad to any FaceTime-enabled device over Wi-Fi or cellular
- Speakers: Landscape stereo speakers
- Microphone: Dual microphones for calls, video recording, and audio recording
- Warranty: One (1) year on parts and service On-Site for the Central Office, Carry-in for the Regional Offices

Below are the minimum specifications of the Five (5) Tablet (For Top-Level Executives) to be procured:
- Wi-Fi + Cellular
- Capacity : 1TB
- With wireless computer keyboard/Magic Keyboard
- With wireless stylus pen accessory
- Size and Weight :
  - 11-inch
  - Wi-Fi + Cellular : 468g
  - Display:
  - Liquid Retina display
  - 11-inch (diagonal) LED-backlit Multi-Touch display with IPS technology
  - 2388-by-1668-pixel resolution at 264 pixels per inch (ppi)
  - ProMotion technology
  - Wide color display (P3)
  - True Tone display
  - Fingerprint-resistant oleophobic coating
  - Fully laminated display
  - Antireflective coating
  - 1.8% reflectivity
  - SDR brightness: 600 nits max
  - Supports Apple Pencil (2nd generation)
  - Apple Pencil hover
- Chip
  - 8-core CPU with 4 performance cores and 4 efficiency cores
  - 10-core GPU
  - 16-core Neural Engine
  - 100GB/s memory bandwidth
  - 16GB RAM on models with 1TB storage
- Camera
  - Pro camera system: Wide and Ultra Wide cameras
  - Wide: 12MP, f/1.8 aperture
  - Ultra Wide: 10MP, f/2.4 aperture, and 125° field of view

- 2x optical zoom out
- Digital zoom up to 5x
- Five-element lens (Wide and Ultra Wide)
- Brighter True Tone flash
- Panorama (up to 63MP)
- Sapphire crystal lens cover
- Autofocus with Focus Pixels (Wide)
- Smart HDR 4
- Wide color capture for photos and Live Photos
- Lens correction (Ultra Wide)
- Advanced red-eye correction
- Photo geotagging
- Auto image stabilization
- Burst mode
- Image formats captured: HEIF and JPEG

- Video Recording
  - 4K video recording at 24 fps, 25 fps, 30 fps, or 60 fps (Wide)
  - 1080p HD video recording at 25 fps, 30 fps, or 60 fps
  - 720p HD video recording at 30 fps
  - ProRes video recording up to 4K at 30 fps (1080p at 30 fps for 128GB storage)
  - 2x optical zoom out
  - Audio zoom
  - Brighter True Tone flash
  - Slo-mo video support for 1080p at 120 fps or 240 fps
  - Time-lapse video with stabilization
  - Extended dynamic range for video up to 30 fps
  - Cinematic video stabilization (4K, 1080p, and 720p)
  - Continuous autofocus video
  - Playback zoom
  - Video formats recorded: HEVC and H.264
  - Stereo recording

- Cellular and Wireless
  - Wi-Fi 6E (802.11ax) with 2x2 MIMO; speeds up to 2.4 Gbps[4]
  - Simultaneous dual band
  - Bluetooth 5.3

- Wi-Fi + Cellular models
  - 5G (sub-6 GHz) with 4x4 MIMO
  - Gigabit LTE with 4x4 MIMO and LAA
  - 5G NR (Bands n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n38, n40, n41, n48, n66, n70, n71, n77, n78, n79)[5]
  - FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 11, 12, 13, 14, 17, 18, 19, 20, 21, 25, 26, 28, 29, 30, 32, 66, 71)
  - TD-LTE (Bands 34, 38, 39, 40, 41, 42, 46, 48)
  - UMTS/HSPA/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)
  - Data only
  - Wi-Fi calling

- eSIM
- True Depth Camera
  - 12MP Ultra Wide camera, 122° field of view
  - $f/2.4$ aperture
  - Portrait mode with advanced bokeh and Depth Control
  - Portrait Lighting with six effects (Natural, Studio, Contour, Stage, Stage Mono, High Key Mono)
  - Animoji and Memoji
  - Smart HDR 4
  - 1080p HD video recording at 25 fps, 30 fps, or 60 fps
  - Time lapse video with stabilization
  - Extended dynamic range for video up to 30 fps
  - Cinematic video stabilization (1080p and 720p)
  - Wide color capture for photos and Live Photos
  - Lens correction
  - Retina Flash
  - Auto image stabilization
  - Burst mode
- Video Calling
  - FaceTime video
  - Center Stage
  - iPad to any FaceTime-enabled device over Wi-Fi or cellular
- Audio Calling
  - FaceTime audio
  - iPad to any FaceTime-enabled device over Wi-Fi or cellular
  - Speakers: Four speaker audio
  - Microphone: Five studio-quality microphones for calls, video recording, and audio recording
- Warranty: One (1) year on parts and service On-Site for the Central Office, Carry-in for the Regional Offices

Below are the minimum specifications of the Eight (8) Server to be procured:
- Processor : Intel Xeon Silver 4310 12C 120W 2.1Ghz
- Memory: 4 x 32GB Tru DDR4 3200 Mhz (2Rx8 1.2V) RDIMM
- Storage: 2.5" PM893 2x480GB read Intensive SATA 6GB HS SSD 2.5" 2.4TB 10K SAS 3x 12GB Hot Swap 512e HDD v2
- Networking: 1 x 4-port 10GBase-T Ethernet Adapter
- External: USB DVD-RW Optical Disk Drive
- Windows Server 2022 Standard ROK (16 core) - MultiLang
- Windows Server CAL 2022 (5 Devices)
- Warranty: Three (3) years on parts and service on sites, 24x7 with 4-hour response time - Keep Your Drive (KYD) retention
- Management Software:

- Must have Quality/Bandwidth control, virtual console chat and virtual console collaboration (six users)
- Must be compliant with NIST SP 800-131A and FIPS 140-2
- Must be able to deploy operating system images to up to 28 bare-metal servers concurrently and should be able to update OS device drivers on deployed operating system.
- Must have REST APIs and a PowerShell Toolkit, Python Toolkit, and Ruby Toolkit, which can be used to automate management functions.

Below are the minimum specifications of the Hyperconverged Infrastructure Solution (Package) to be procured:
- Nodes: 3
- Type: Rackmount
- Processor: 1 x Intel Xeon Gold 5416S 16C 150W 2.0Ghz
- Memory: 8 x 32GB Tru DDR5 4800Mhz RDIMM memory Must offer protection in the event of a non-correctable memory failure, Adaptive Double Device Data Correction, Error correction code (ECC), memory mirroring, and memory rank sparing, patrol scrubbing, and demand scrubbing
- Storage: Eight (8) x 960GB SATA 6Gb Hot Swap SSD
  Two (2) x 960GB NVMe PCIe Non-Hot Swap SSD
- Power Supply: 2 x Hot-Swap 1100W power supply
- Network Interface: 4-port 10GbE Base-T
  2-port 10/25GbE SFP28 with transceivers
- Hot-Swap Components: HDD, Power Supply, and System Fans
- HCI Software must be capable of:
  - Be capable of Heterogeneous Clusters
  - Be capable of Data Tiering
  - Be capable of Online Cluster Grow/Shrink
  - Be capable of Data Path Redundancy
  - Tunable Redundancy Factor of, "2 or 3"
  - Availability Domains: Node, Block, Rack
  - Be capable of Basic Compression - Inline and post process
  - Be capable of Deep Compression - Greater efficiency for cold data
  - Be capable of Data Deduplication
  - Be capable of Erasure Coding (EC-X)
  - Be capable of VM Centric Storage QoS
  - Be capable of VM Flash Mode
  - Be capable of Volume Groups – for In-cluster VMs
  - Be capable of Volume Groups - external access
  - Be capable of Self-Service Restore
  - Be capable of Multiple Site DR
  - Be capable of Client Authentication
  - Be capable of Cluster Lockdown
  - Be capable of HA Guaranteed Failover
  - Be capable of VM-Host Affinity Policies

- HCI Management must be capable of:
  - Reporting
  - Capacity Forecast and Planning
  - Resource Inefficiency Detection and Right-sizing
  - Support for ESXi on non-native Environments
  - Low-code/No-code Operations Automation
  - SQL Server Monitoring for IT Ops
  - Application Discovery
  - Self-tuning with Machine Learning
  - Cost metering for private cloud resources
  - Cloud Visibility and Optimization
  - Self-Service Marketplace
  - IaaS (Single VM) Blueprints
  - Advanced Orchestration Runbooks

- Two (2) Top-of the-rack switch
  - 24 x 100M/1/2.5/5/10GBASE-T 802.3bt (90W) ports
    - Full-Duplex
    - MACsec-capable
  - 30W, 60W, and 90W PoE support for powering Ethernet connecte devices
  - Non-blocking wire speed design
  - 2x Stacking/QSFP28 ports
  - 6x 1Gb/10Gb/25Gb SFP28 MACsec-capable ports
  - 1x Serial console port (RJ-45)
  - 1x 10/100/1000BASE-T out-of-band management port
  - 2x USB A ports for management or external USB flash
  - 1x USB Micro-B console port
  - 1 x SSD slot
  - Hot-swappable, redundant power supplies and fans
  - 1280 Gbps Aggregated Switch Bandwidth
  - 810 mpps Frame Forwarding Rate
  - 3 Years Warranty
- Other Requirements:
  - Switch vendors should be listed as leaders in the Gartner Magic Quadrant Report for Enterprise Wired and Wireless LAN Infrastructure for at least the past three years.
  - Switch should have a Cloud-Based Network Management (3 Years subscription and support)
  - Cloud-Based Network Management must support enhanced policy enforcement, visibility, reporting, and advanced configurations. Delivers configuration and management of infrastructure devices at scale including advanced policy, advanced segmentation, advanced troubleshooting, advanced guest, advanced SSH, etc.
  - Supports a dual-persona capability, allowing you to choose your OS. Either stacking or fabric services can be selected at switch start-up or

changed at a later stage. When selected, the switch assumes the features and capabilities of that OS. OS selection can also be automated with Cloud-Based Network Management so that the desired OS can be automatically loaded at switch start-up, facilitating remote OS enablement.

- Stacking OS must support high-speed 400Gb stacking capabilities with the ability to stack up to eight units.
- Stacking OS must support the ability to authenticate multiple users on a single port via 802.1X, web, or MAC at the same time.
- Stacking OS must support Denial of Service (DoS) protection. Stacking OS must support the ability to automatically connect to the fabric backbone. Please describe the available features.
- Fabric OS must support standards based supporting IEEE 802.1aq Shortest Path Bridging (SPB), as well as IETF RFC 6329 to extend fabric services to the network edge.
- Fabric OS must support a built-in functionality to extend IEEE 802.1aq fabric solution over an IP infrastructure.
- Fabric OS must support a web-management interface that can be used to monitor and manage the device through a supported Web browser from anywhere on the network.
- . Must have 3 years warranty, 24x7 with 4-hour response time.
- Support for hypervisor should have direct routing to senior-level engineers.
- Should have the capability to contact support through a single route, 24/7, for any hardware or software concerns. The support platform should include phone support, chat support and service request.
- Must provide administrator's training for three (3) technical personnel of MARINA.
- Training must be conducted by a Certified Training expert for the solution being offered
- Must have a support phone number, live chat and Service Request that will support both hardware and software using a single platform. Hardware and Software must have a single point of contact from the manufacturer's local office (Philippines).

Below are the minimum specifications of the One (1) Firewall Security Appliance to be procured:
- 3 Years Subscription
- Form Factor : 1U Rackmount
- Processor : x86 AMD CPU
- NPU Processor: Marvell NPU
- CPU Memory: 16 GB (2666) DDR4
- NPU Memory : 4GB DDR4
- Storage : 1x min. 240 GB SATA-III
- Ports : 8 x GE copper | 2 x SFP Fiber | 2x SFP+ 10GE Fiber

- I/O Ports : 2x USB 3.0 | 1x USB 2.0 | 1x RJ45 MGMT | 1x COM RJ45 , 1x Micro USB (cable included) | 1x expansion slot
- Display : Multi-function LCD display
- Power Supply : Internal auto-ranging DC 100-240VAC, 3-6A@50-60 Hz, Optional External Redundant PSU
- Product Certifications (Safety, EMC) : CB, CE, UL, FCC, ISED, VCCI, CCC,KC, BSMI, RCM, NOM, Anatel
- Security Performance
  - Firewall Throughput : 58,000 Mbps
  - Firewall IMIX: 27,000 Mbps
  - Firewall Latency (64 byte UDP): 4 µs
  - IPsec VPN throughput: 31,100 Mbps
  - IPsec VPN concurrent tunnels: 6,500
  - IPS throughput : 14,000 Mbps
  - Threat Protection throughput : 3,000 Mbps
  - Latency: (64 BYTE UDP) 5 µs
  - NGFW: 12,500 Mbps
  - Concurrent connections : 13,700,000
  - New connections/sec : 257,800
  - SSL/TLS Inspection: 3,130 Mbps
  - SSL/TLS Concurrent connections: 102,400
  - Maximum licensed users : unrestricted
- General Management
  - Purpose-built, streamlined user interface and firewall rule management for large rule sets with grouping with at-a-glance rule feature and enforcement indicators
  - Two-factor authentication (One-time-password) support for administrator access, user portal, IPSec and SSL VPN for additional security
  - Must be capable of High Availability (HA) support clustering two devices in active-active or active-passive mode with plug-and-play Quick HA setup
  - Full command-line-interface (CLI) accessible from GUI
  - Role-based administration
  - Automated firmware update notification with easy automated update process and roll-back features
  - Reusable system object definitions for networks, services, hosts, time periods, users and groups, clients and servers
  - Central management support via Cloud-based Unified Console
  - Automatic Email Notifications for any important event
  - Backup and restore configurations: locally, via FTP or email; on-demand, daily, weekly, or monthly
  - Supports a broad range of virtualization platforms and can also be deployed as a software appliance
  - on your own x86 Intel hardware

- Centralized Firewall Management
  - Cloud-based management and reporting for multiple firewalls provides group policy management and a single console
  - Group policy management allows objects, settings, and policies to be modified once and automatically synchronized to all firewalls in the group
  - Task Manager provides a full historical audit trail and status monitoring of group policy changes
  - Backup firmware management which stores the last five configuration backup files for each firewall with one that can be pinned for permanent storage and easy access
  - Capable of Firmware update scheduling
  - Multi-firewall reporting across firewall groups
- Firewall, Networking & Routing
  - Stateful deep packet inspection firewall
  - All firewall rules provide an at-a-glance summary of the applied security and control for AV, sandboxing, IPS, Web, App, Traffic Shapping (QoS), and Heartbeat
  - Packet processing architecture that provides extreme levels of visibility, protection, and performance through stream-based packet processing
  - Zone-based firewall
  - SD-WAN link balancing: multiple Internet connections, auto-link health check, automatic failover, automatic and weighted balancing, and granular multipath rules
  - Wireless WAN support (n/a in virtual deployments)
  - 802.3ad interface link aggregation
  - Full configuration of DNS, DHCP and NTP
  - Dynamic DNS (DDNS)
  - IPv6 Ready Logo Program Approval Certification
  - IPv6 tunnelling support including 6in4, 6to4, 4in6, and IPv6 rapid deployment (6rd) through IPSec
- Base Traffic Shaping & Quotas
  - Flexible network or user based traffic shaping (QoS) (enhanced Web and App traffic shaping options
- Authentication
  - Verifies User Identity based on the Active Directory active user list between endpoints and the firewall without an agent on the AD server or client
  - Authentication certificates for iOS and Android
  - Authentication services for IPsec, SSL, L2TP, PPTP
  - Google Chromebook authentication support for environments with Active Directory and Google G Suite
  - API-based authentication
  - Must support external authentication via: Active Directory, eDirectory, RADIUS, LDAP and TACACS+

28

- Authentication
  - Verifies User Identity based on the Active Directory active user list between endpoints and the firewall without an agent on the AD server or client
  - Authentication certificates for iOS and Android
  - Authentication services for IPsec, SSL, L2TP, PPTP
  - Google Chromebook authentication support for environments with Active Directory and Google G Suite
  - API-based authentication
  - Must support external authentication via: Active Directory, eDirectory, RADIUS, LDAP and TACACS+
- User Self-Serve Portal
  - Must have a separate user portal where network users can manage their credentials, VPN client download, access quarantined emails and monitor their internet usage without having to call in an administrator or product support.
- Base VPN Options
  - Remote VPN user must be able to download VPN client and configuration via a secured web based application and must be capable of using two-factor authentication to ensure a higher level of security of access.
  - Must support multiple VPN options (PPTP, L2TP, IPsec, SSL)
  - Remote Access VPN with a free and easy client for Windows/Macs
  - VPN users must be able to authenticate either from local user database or from external user database
- Intrusion Prevention (IPS)
  - High-performance, next-gen IPS deep packet inspection engine with selective IPS patterns that can be applied on a firewall rule basis for maximum performance and protection
  - Must have Zero-day threat protection against zero-day malware
  - IPS Policy Smart Filters enable dynamic policies that automatically update as new patterns are added
- ATP and Security
  - Advanced Persistent Threat Protection (detect and block network traffic attempting to contact command and control servers using multi-layered DNS, AFC, and firewall)
  - User Threat Quotient identifies risky users based on recent browsing behaviour and ATP triggers
- VPN Client
  - Intelligent split-tunneling for optimum traffic routing
  - Client-monitor for graphical overview of connection status
  - Mac (IPsec) and Windows (SSL/IPsec) client support
  - NAT-traversal support
  - Must support Authentication: Pre-Shared Key (PSK), PKI (X.509), Token and XAUTH

- Web Protection and Application Control
  - Fully transparent proxy for anti-malware and web-filtering with over 90 categories that can be allowed, denied or warned access by the policy administrator.
  - Should support Dual engine anti-virus scanning to eliminate false positives and ensure a positive web security for users against from all forms of viruses, web malware, trojans and spyware on HTTP/S, FTP and web-based email and should detect and block potentially unwanted software.
  - Malware scanning: block all forms of viruses, web malware, trojans, and spyware on HTTP/S, FTP and web-based email
  - Must be capable of forced caching for endpoint updates and web contents
  - Policy test simulator tool enables firewall rule and web policy simulation and testing by user, IP, and time of day
  - Access time polices per user/group
  - Real-time or batch mode scanning
  - Live Protection real-time, in-the-cloud lookups for the latest threat intelligence
  - Must supports Pharming protection
  - Enforce tenant restrictions for O365
  - High performance web content caching
  - SSL protocol tunnelling detection and enforcement
  - Surfing quota time policies per user/group
  - File type filtering by mime-type, extension, and active content types e.g. Activex, applets, cookies, etc.)
- Cloud Based Reporting
  - Must be able to support integration on cloud based platform for firewall management and be capable of generating reports and keep at least 7 days of reporting without additional cost for using the platform or data retention. But with an optional cost to expand storage capability for additional data storage and retention
- Warranty and Support
  - Hardware warranty & RMA with Advanced Exchange
  - 24x7 Enhanced Plus Support via Telephone & Email with Remote Consultation from STSE (up to 4 hrs)
  - FREE Security Updates & Patches
  - FREE Software Features Updates & Upgrades
- Additional Protection Modules
  - Email Protection: On-box antispam, AV, DLP, encryption
  - Web Server Protection: Web Application Firewall
  - Consultation from STSE (up to 4 hrs)

H. DOCUMENTATION

The winning bidder must provide complete technical and system documentation for every deliverable. All documentation must be written in English and be available in both soft and paper formats.

I. TRANSFER OF TECHNOLOGY

Training for ten (10) participants for one (1) day based on the following:
1. Basic Troubleshooting and installation on Desktop, Laptops and Servers
2. Appropriate manuals (e.g. Equipment, User and Operational Manuals) shall be provided to each participant.
3. Training and technology transfer should be conducted before final project acceptance.
4. All expenses incurred during the training shall be borne by the winning bidder.

J. TERMS OF PAYMENT

The payment shall be made upon issuance of Billing Statement on a Bank-to-Bank- basis. Automatic Debit Arrangement (ADA) though Land Bank of the Philippines (LBP) facilities, for other Commercial bank, applicable bank charges shall be for the account of the winning bidder. The winning bidder shall submit bank details together with the billing statement/invoice for ready reference.
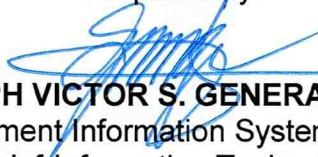
K. Delivery Schedule

The various ICT equipment must be delivered within one hundred and twenty (120) days, upon receipt of the Notice to Proceed (NTP), to MARINA Central Office and Regional Offices. (as included in below table)

ICT Equipment		MRO 1 & 2	MRO IV	MRO V	MRO VI	MRO VII	MRO VIII	MRO IX	MRO X	MRO XI	MRO XII	MRO XIII	MARINA CENTRAL OFFICE
All-in-One Desktop													31
Desktop		13	39	19	28	40	33	20	21	22	18	16	481
High-end Desktop for Production (Video and Graphics Design)													5
Laptop		2	2	2	2	2	2	2	2	2	2	2	40
Laptop for Production (Video and Graphics Design)													3

Laptop (For Division Chiefs and Directors)		2	2	2	2	2	2	2	2	2	2	2	44
Laptop (For Programmers)													10
Tablet (For Engineers)		2	3	3	8	8	8	3	3	3	3	3	13
Tablet (For Top-Level Executives)													5
Server													8
Hyperconverged Infrastructure Solution													1
Firewall Security Appliance													1
Total ICT equipment to be delivered to MROs and CO		19	46	26	40	52	45	27	28	29	25	23	642

Prepared by:

JOSEPH VICTOR S. GENERATO PhD
Management Information Systems Service
Division Chief-Information Technology Division

Recommending Approval:

LINA Y. MAQUERA
Management Information Systems Service
OIC-Director

Reviewed by:

JOHN GUARDAYA
Head, TWG-IT

Atty. SHARON D. ALEDO
Chairperson, BAC

Approved by:

Atty. HERNANI N. FABIA
Administrator

33