



Bid Notice Abstract

Request for Quotation (RFQ)

Reference Number 8171408
Procuring Entity MARITIME INDUSTRY AUTHORITY (MARINA)
Title SUPPLY, DELIVERY, INSTALLATION AND CONFIGURATION OF NETWORK MONITORING SYSTEM (SUBSCRIPTION) – 3rd Posting
Area of Delivery Metro Manila

Solicitation Number:	2021-07-308	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 750,000.00		
Delivery Period:	30 Day/s	Document Request List	0
Client Agency:			
Contact Person:	VADM Rene V. Medina AFP (Ret) The BAC Chairperson c/o BAC Office, 10th Floor, MARINA Bldg. A. Bonifacio Drive cor. 20th Street, Port Area Manila Metro Manila Philippines 1018 63-2-85246518 2021marinabac@gmail.com	Date Published	10/11/2021
		Last Updated / Time	09/11/2021 16:28 PM
		Closing Date / Time	15/11/2021 13:00 PM
Description SUPPLY, DELIVERY, INSTALLATION AND CONFIGURATION OF NETWORK MONITORING SYSTEM (SUBSCRIPTION) – 3rd Posting 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 09/11/2021

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.



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 NETWORK MONITORING SYSTEM (SUBSCRIPTION) – 3rd Posting** for FY 2021 in accordance with Section 53.9 of the 2016 Revised Implementing Rules and Regulation of Republic Act No. 9184.

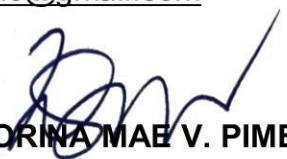
Please quote your **best offer** for the item described herein, **subject to the Terms and Conditions** provided at the last page of this Request for Quotation (RFQ). Submit your quotation duly signed by you or your representative **not later than (15 November 2021, 01:00 P.M.)** at the MARINA BAC Office, located at 10th Floor MARINA Building, Bonifacio Drive cor. 20th Street, Port Area, Manila, Philippines.

Qualification of the supplier: The supplier must be **legally registered**, and has at **least 1 experience in supplying Network Monitoring System within the last 3 years**.

A copy of your **2021 Business/Mayor's Permit¹, 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 the proposed Network Monitoring System** and **submit atleast two (2) Client Satisfactory Certificates**.

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


ATTY. KORINA MAE V. PIMENTEL
Head, BAC Secretariat

¹ In case of recently expired Mayor's/Business permit, it shall be accepted together with its official receipt as proof that The Supplier 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:

INSTRUCTIONS:

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

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

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 NETWORK MONITORING SYSTEM (SUBSCRIPTION) – 3rd Posting		
Code	Specifications	Supplier's Statement of Compliance
A	TECHNICAL SPECIFICATION 1. The Monitoring Solution should provide Unified Architectural design offering seamless common functions including but not limited to: a. Event and Alarm management, b. Auto-discovery of the IT environment, c. Performance and availability managemen d. Service Level Management, notifications e. Reporting and analytics f. Automation and Customization 2. Should be a tight integration between infrastructure metrics and logs to have the single consolidated console of Infrastructure & security events. 3. Should be able to pull up security events related to a given Configuration Item, from a single console which also has NOC events, and use the security events to triage the problem. This way the Operator gets consolidated system/network event details and security events (current and historical) from the same console and save time in troubleshooting / isolating the issue. 4. Should be able to build correlation rules in a simple GUI based environment where the Operator should be able to correlate cross domain events 5. Shall provide future scalability of the whole system without major architectural changes. 6. Shall be distributed, scalable, and multi-platform and open to third party integration such as Cloud, Virtualization, Database, Web Server, Application Server platforms etc. 7. All the required modules should be from same OEM and should be tightly integrated for single pane of glass view of enterprise monitoring 8. Must provide single integrated dashboard to provide line of business views and drill down capabilities to navigate technical operators right from services to last infrastructure components 9. Consolidated dashboard of the proposed NMS solution must be able to do dynamic service modelling of all business-critical production services & use near-real time Service Model for efficient cross domain event correlation. 10. Must provide SDK/Rest API for North bound and South Bound Integrations e.g. Forwarding specific metric data to third party database, Notifications to third party systems such as Jira, AutoDesk, Slack	

Signature over Printed Name

Position/Designation

B	DETAILED SPECIFICATIONS 1. Must provide complete cross-domain visibility of IT infrastructure issues 2. Must consolidate monitoring events from across layers such as Network, Server, Application, Database etc 3. Should support single console for automated discovery of enterprise network components e.g. network device, servers, virtualization, cloud, application and databases 4. Must support custom dashboards for different role users such as Management, admin and report users 5. Must allow creating custom data widget to visualize data with user preferences ex. Refresh time, time span, background color, unit conversion 6. Must support multiple visualization methods such as gauge, grid, charts, Top N etc. 7. Should provide superior view of infrastructure health across system, networks, application and other IT Infrastructure components into a consolidated, central console 8. There should be only one dashboard/interface to collected network/server/ application/log data after correlation and consolidation across the IT landscape to reduce/correlate number of metrics/alerts	
C	NETWORK PERFORMANCE MANAGEMENT 1. Shall provide a single integrated solution for comprehensive management of the wired/wireless access, and rich visibility into connectivity and performance assurance issues. 2. Shall facilitate creation of templates used for monitoring key network resources, devices, and attributes. Default templates and best practice designs are provided for quick out-of-the-box implementation automating the work required to use OEM validated designs and best practices. 3. Must provide comprehensive and integrated management of IT infrastructure components to maximize the availability of IT services and SLA performance. 4. Must provide the complete view of the Topology and network elements. The NMS shall have the ability to include the network elements and the links in the visual/graphical map of the department. The visual maps shall display the elements in different color depending upon the status of the element. It is preferable that green color for healthy and amber/yellow color for degraded condition and red for unhealthy condition is used. 5. Must have suitable system level backup mechanism for taking backup of NMS data manually as well as automatically 6. Must keep historical data at raw level without averaging for minimum of six month 7. Must provide the visual presentation of the Network Element's status and the alarms. It shall also present the complete map of the network domain with suitable icons and in suitable color like green for healthy, red for non-operational, yellow for degraded mode of operation etc. 8. Must provide Health Monitoring reports of the network with settable periodicity –(24 Hrs, 1 week, 1 month) with no limit of time frame. 9. Must provide the graphical layout of the network element with modules drawn using different colors to indicate their status 10. Must provide calendar view which allows the operator all the schedule activities such as Reports, Inventory scans etc. It shall also allow to define scheduled report for uptime, link status etc. 11. Should have multiple alerting features to get the notification via email, sms and third-party systems 12. Must support listening to traps and syslog events from the network devices with no limit on retention period. 13. Must support defining the data retention period to control storage 14. Must support custom device template to support Generic SNMP devices 15. Must provide discovery & inventory of heterogeneous physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices and do mapping of LAN & WAN connectivity with granular visibility up to individual ports level. 16. Shall provide Real time network monitoring and Measurement off-end-to-end Network performance & availability to define service levels and further improve upon them.	

Signature over Printed Name

Position/Designation

D	FAULT MANAGEMENT	
	1. Must provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis. It should also have a strong event correlation engine which can correlate the events on the basis of event pairing, event sequencing etc. 2. Must include an event correlation automatically fed with events originating from managed elements, monitoring tools or data sources external to the platform. This correlation must perform: a. Event filtering b. Event suppression c. Event aggregation d. Event annotation 3. Must support creating and monitoring of rising or falling thresholds with respect to basic key performance indicators for network, system and application infrastructures. 4. Should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis. It should also have a strong event correlation engine which can correlate the events on the basis of event pairing, event sequencing etc. 5. Must have powerful correlation capabilities to reduce number of actionable events. Topology based and event stream-based correlation should be made available. 6. Must offer relevant remedy tools, graphs in context of a selected fault alarm/event 7. Should have capability to configure actions-based rules for set of pre-defined alarms/alerts enabling automation of set tasks. 8. Must support Event or Alarm Correlation integrations with service desk to trigger automated creation of incidents, problems management 9. Should classify events based on business impact and also allow defining custom severity levels and priority metrics such as Ok, Critical, Major, Down, Info etc with color codes 10. Should allow creation of correlation or analytics rules for administrators 11. Must provide default event dashboard to identify, accept and assign generated alarms	

Signature over Printed Name

Position/Designation

E	LOG MANAGEMENT	
	1. Must provide a common classification of event irrespective of the log format 2. Must provide the ability to store/ retain both normalized and the original raw format of the event log as for forensic purposes without any time limit and allow to extend it to further with additional hardware without any disruption to the ongoing data collection 3. The proposed solution should provide a minimum log compression of 8:1 for ensuring log compression to reduce overall log index storage space for the raw log format 4. The log data generated should be stored in a centralized server. The period upto which the data must be available should be customizable. 5. Must support logs collected from commercial and proprietary applications. For assets not natively supported, the solution should provide the collection of events through customization of connectors or similar integration 6. Must support log collection for Directories (i.e. AD, LDAP), hosted applications such as database, web server, file integrity logs etc. using agents 7. The Log receiver or log collection component must store the data locally if communication with centralized collector/receiver is unavailable. 8. Must support log collection from Network infrastructure (i.e. switches, routers, etc.). Please describe the level of support for this type of product. 9. The system shall support the following log formats for log collection: a. Windows Event Log b. Syslog c. Access Log Data d. Application Log data e. Any Custom Log data f. Text Log (flat file) g. JSON Data 10. Should be able to collect raw logs in real-time to a Central log database from any IP device including: a. Networking devices(router/switches/voice gateways) b. Security devices (IDS/IPS, AV, Patch Mgmt., Firewall/DB Security solutions) c. Operating systems(Windows 2003/2008,Unix,linux,AIX) d. Virtualization Platforms(Microsoft HyperV, VMware Vcenter/VSphere, 4.X, vDirector, Citrix) e. Databases(Oracle/SQL/MYSQL/DB2) 11. Should support collection of logs through Syslog, syslogNG and also provide native Windows Agents as well as Agentless(PowerShell) connectors 12. Must provide alerting based upon established policy 13. Must provide SDK and Rest API to write custom connectors and collectors to pull log and monitoring data from third party system 14. Must provide UI based wizard and capabilities to minimize false positives and deliver accurate results. 15. Must collect, index the log messages and support full-text searching for forensic investigation 16. Must support the ability to take action upon receiving an alert. For example, the solution should support the ability to initiate a script or send an email message. 17. Must provide pre-defined log correlation rules to detect suspicious behavior 18. The solution must support real-time and scheduled alerting time-line while creating a log policy to catch specific log pattern 19. Should support applying regex pattern in real-time to extract vendor specific log data for reporting and alerting purpose 20. Shall have the capability to drag and drop building of custom search queries & reports 21. Shall be capable of operating at a sustained 5000 EPS per collection instance. 22. Shall provide the ability to scale to higher event rates by adding multiple collection instance	
F	ROLE-BASED ACCESS CONTROL	
	1. Should have inbuilt role-based access module to enable multiple users with different groups to create dashboards specific to their department 2. Should have way to control and define permission such as read/write for set of devices rather than all the devices for the ease of use.	

Signature over Printed Name

Position/Designation

G	OTHER KEY REQUIREMENTS 1. Should provide all the modules as a single monitoring engine to correlate events in real-time from Networks, Servers and Applications 2. Should be virtual appliance and deployable on Linux operating systems to reduce the overall TCO 3. Should have built-in time series database support for better response time, retention and analytics support. 4. Should have plugin driven architecture for easy integrations and monitoring of devices. 5. Must have bundled annual Branded SMS gateway with 10,000 credits 6. Must provide native Windows Agents as well as Agentless (PowerShell) connectors	
H	SUPPORT 1. The Supplier shall provide daily 8 by 5 phone, email, and remote support with critical level on site assistance 2. The Supplier must have access to high-level of support via the principal for critical level concerns 3. The Supplier must provide professional implementation services 4. The Supplier must provide a monthly health check during the subscription period to ensure that the product is properly working 5. The Supplier 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.	
I	WARRANTY The warranty shall be for a period of One (1) year.	
J	OTHERS 1. The winning Supplier is required to conduct a requirements analysis for the configuration of the whole setup within 15 calendar days after issuance of Notice to Proceed. The Supplier must submit complete documentation of the entire work plan, resource (hw/sw) requirements, manpower requirements, network design, course syllabus (for knowledge transfer) etc. 2. The winning Supplier 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. 3. At the end of the implementation phase, the winning Supplier must submit a comprehensive documentation on the final setup. The documentation should include a network / logical diagram, configuration settings, and all manuals.	
UNIT COST		TOTAL COST

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

Signature over Printed Name

Position/Designation

SUPPLY, DELIVERY, INSTALLATION AND CONFIGURATION OF NETWORK MONITORING SYSTEM (SUBSCRIPTION) – 3rd Posting	
PAYMENT	Supplier's's Statement of Compliance
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 the Commercial Bank, applicable bank charges shall be for the account of supplier. The supplier submit bank details together with billing statement/invoice for ready reference.	

Signature over Printed Name

Position/Designation

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 NETWORK MONITORING SYSTEM (SUBSCRIPTION) – 2nd Posting		
Code	Specifications	Delivery Date**
A	TECHNICAL SPECIFICATION - The Monitoring Solution should provide Unified Architectural design offering seamless common functions including but not limited to: - Event and Alarm management, - Auto-discovery of the IT environment, - Performance and availability management - Service Level Management, notifications - Reporting and analytics - Automation and Customization - Should be a tight integration between infrastructure metrics and logs to have the single consolidated console of Infrastructure & security events. - Should be able to pull up security events related to a given Configuration Item, from a single console which also has NOC events, and use the security events to triage the problem. This way the Operator gets consolidated system/network event details and security events (current and historical) from the same console and save time in troubleshooting / isolating the issue. - Should be able to build correlation rules in a simple GUI based environment where the Operator should be able to correlate cross domain events - Shall provide future scalability of the whole system without major architectural changes. - Shall be distributed, scalable, and multi-platform and open to third party integration such as Cloud, Virtualization, Database, Web Server, Application Server platforms etc. - All the required modules should be from same OEM and should be tightly integrated for single pane of glass view of enterprise monitoring - Must provide single integrated dashboard to provide line of business views and drill down capabilities to navigate technical operators right from services to last infrastructure components - Consolidated dashboard of the proposed NMS solution must be able to do dynamic service modelling of all business-critical production services & use near-real time Service Model for efficient cross domain event correlation. - Must provide SDK/Rest API for North bound and South Bound Integrations e.g. Forwarding specific metric data to third party database, Notifications to third party systems such as Jira, AutoDesk, Slack	The winning supplier is required to deliver and deploy the solution within 30 calendar days after issuance of Notice to Proceed
B	DETAILED SPECIFICATIONS - Must provide complete cross-domain visibility of IT infrastructure issues - Must consolidate monitoring events from across layers such as Network, Server, Application, Database etc - Should support single console for automated discovery of enterprise network components e.g. network device, servers, virtualization, cloud, application and databases - Must support custom dashboards for different role users such as Management, admin and report users - Must allow creating custom data widget to visualize data with user preferences ex. Refresh time, time span, background color, unit conversion - Must support multiple visualization methods such as gauge, grid, charts, Top N etc. - Should provide superior view of infrastructure health across system, networks, application and other IT Infrastructure components into a consolidated, central console - There should be only one dashboard/interface to collected network/server/ application/log data after correlation and consolidation across the IT landscape to reduce/correlate number of metrics/alarms	

Signature over Printed Name

Position/Designation

C	NETWORK PERFORMANCE MANAGEMENT 1. Shall provide a single integrated solution for comprehensive management of the wired/wireless access, and rich visibility into connectivity and performance assurance issues. 2. Shall facilitate creation of templates used for monitoring key network resources, devices, and attributes. Default templates and best practice designs are provided for quick out-of-the-box implementation automating the work required to use OEM validated designs and best practices. 3. Must provide comprehensive and integrated management of IT infrastructure components to maximize the availability of IT services and SLA performance. 4. Must provide the complete view of the Topology and network elements. The NMS shall have the ability to include the network elements and the links in the visual/graphical map of the department. The visual maps shall display the elements in different color depending upon the status of the element. It is preferable that green color for healthy and amber/yellow color for degraded condition and red for unhealthy condition is used. 5. Must have suitable system level backup mechanism for taking backup of NMS data manually as well as automatically 6. Must keep historical data at raw level without averaging for minimum of six month 7. Must provide the visual presentation of the Network Element's status and the alarms. It shall also present the complete map of the network domain with suitable icons and in suitable color like green for healthy, red for non-operational, yellow for degraded mode of operation etc. 8. Must provide Health Monitoring reports of the network with settable periodicity –(24 Hrs, 1 week, 1 month) with no limit of time frame. 9. Must provide the graphical layout of the network element with modules drawn using different colors to indicate their status 10. Must provide calendar view which allows the operator all the schedule activities such as Reports, Inventory scans etc. It shall also allow to define scheduled report for uptime, link status etc. 11. Should have multiple alerting features to get the notification via email, sms and third-party systems 12. Must support listening to traps and syslog events from the network devices with no limit on retention period. 13. Must support defining the data retention period to control storage 14. Must support custom device template to support Generic SNMP devices 15. Must provide discovery & inventory of heterogeneous physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices and do mapping of LAN & WAN connectivity with granular visibility up to individual ports level. 16. Shall provide Real time network monitoring and Measurement of end-to-end Network performance & availability to define service levels and further improve upon them.	The winning supplier is required to deliver and deploy the solution within 30 calendar days after issuance of Notice to Proceed
D	FAULT MANAGEMENT 1. Must provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis. It should also have a strong event correlation engine which can correlate the events on the basis of event pairing, event sequencing etc. 2. Must include an event correlation automatically fed with events originating from managed elements, monitoring tools or data sources external to the platform. This correlation must perform: a. Event filtering a. Event suppression b. Event aggregation c. Event annotation 3. Must support creating and monitoring of rising or falling thresholds with respect to basic key performance indicators for network, system and application infrastructures. 4. Should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis. It should also have a strong event correlation engine which can correlate the events on the basis of event pairing, event sequencing etc. 5. Must have powerful correlation capabilities to reduce number of actionable events. Topology based and event stream-based correlation should be made available. 6. Must offer relevant remedy tools, graphs in context of a selected fault alarm/event 7. Should have capability to configure actions-based rules for set of pre-defined alarms/alerts enabling automation of set tasks. 8. Must support Event or Alarm Correlation integrations with service desk to trigger automated creation of incidents, problems management 9. Should classify events based on business impact and also allow defining custom severity levels and priority metrics such as Ok, Critical, Major, Down, Info etc with color codes 10. Should allow creation of correlation or analytics rules for administrators 11. Must provide default event dashboard to identify, accept and assign generated alarms	

Signature over Printed Name

Position/Designation

E	LOG MANAGEMENT 1. Must provide a common classification of event irrespective of the log format 2. Must provide the ability to store/ retain both normalized and the original raw format of the event log as for forensic purposes without any time limit and allow to extend it to further with additional hardware without any disruption to the ongoing data collection 3. The proposed solution should provide a minimum log compression of 8:1 for ensuring log compression to reduce overall log index storage space for the raw log format 4. The log data generated should be stored in a centralized server. The period upto which the data must be available should be customizable. 5. Must support logs collected from commercial and proprietary applications. For assets not natively supported, the solution should provide the collection of events through customization of connectors or similar integration 6. Must support log collection for Directories (i.e. AD, LDAP), hosted applications such as database, web server, file integrity logs etc. using agents 7. The Log receiver or log collection component must store the data locally if communication with centralized collector/receiver is unavailable. 8. Must support log collection from Network infrastructure (i.e. switches, routers, etc.). Please describe the level of support for this type of product. 9. The system shall support the following log formats for log collection: a. Windows Event Log b. Syslog c. Access Log Data d. Application Log data e. Any Custom Log data f. Text Log (flat file) g. JSON Data 11. Should be able to collect raw logs in real-time to a Central log database from any IP device including: a. Networking devices (router/switches/voice gateways) b. Security devices (IDS/IPS, AV, Patch Mgmt., Firewall/DB Security solutions) c. Operating systems (Windows 2003/2008, Unix, linux, AIX) d. Virtualization Platforms (Microsoft HyperV, VMware Vcenter/VSphere, 4.X, vDirector, Citrix) e. Databases (Oracle/SQL/MYSQL/DB2) 23. Should support collection of logs through Syslog, syslogNG and also provide native Windows Agents as well as Agentless (PowerShell) connectors 24. Must provide alerting based upon established policy 25. Must provide SDK and Rest API to write custom connectors and collectors to pull log and monitoring data from third party system 26. Must provide UI based wizard and capabilities to minimize false positives and deliver accurate results. 27. Must collect, index the log messages and support full-text searching for forensic investigation 28. Must support the ability to take action upon receiving an alert. For example, the solution should support the ability to initiate a script or send an email message. 29. Must provide pre-defined log correlation rules to detect suspicious behavior 30. The solution must support real-time and scheduled alerting time-line while creating a log policy to catch specific log pattern 31. Should support applying regex pattern in real-time to extract vendor specific log data for reporting and alerting purpose 32. Shall have the capability to drag and drop building of custom search queries & reports 33. Shall be capable of operating at a sustained 5000 EPS per collection instance. 34. Shall provide the ability to scale to higher event rates by adding multiple collection instance	The winning supplier is required to deliver and deploy the solution within 30 calendar days after issuance of Notice to Proceed
F	ROLE-BASED ACCESS CONTROL 1. Should have inbuilt role-based access module to enable multiple users with different groups to create dashboards specific to their department 2. Should have way to control and define permission such as read/write for set of devices rather than all the devices for the ease of use.	
G	OTHER KEY REQUIREMENTS 1. Should provide all the modules as a single monitoring engine to correlate events in real-time from Networks, Servers and Applications 2. Should be virtual appliance and deployable on Linux operating systems to reduce the overall TCO 3. Should have built-in time series database support for better response time, retention and analytics support. 4. Should have plugin driven architecture for easy integrations and monitoring of devices. 5. Must have bundled annual Branded SMS gateway with 10,000 credits 6. Must provide native Windows Agents as well as Agentless (PowerShell) connectors	
H	SUPPORT 1. The Supplier shall provide daily 8 by 5 phone, email, and remote support with critical level on site assistance 2. The Supplier must have access to high-level of support via the principal for critical level concerns 3. The Supplier must provide professional implementation services 4. The Supplier must provide a monthly health check during the subscription period to ensure that the product is properly working 5. The Supplier 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.	
I	WARRANTY The warranty shall be for a period of One (1) year.	

Signature over Printed Name

Position/Designation

J	OTHERS 1. The winning Supplier is required to conduct a requirements analysis for the configuration of the whole setup within 15 calendar days after issuance of Notice to Proceed. The Supplier must submit complete documentation of the entire work plan, resource (hw/sw) requirements, manpower requirements, network design, course syllabus (for knowledge transfer) etc. 2. The winning Supplier 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. 3. At the end of the implementation phase, the winning Supplier must submit a comprehensive documentation on the final setup. The documentation should include a network / logical diagram, configuration settings, and all manuals.	The winning supplier is required to deliver and deploy the solution within 30 calendar days after issuance of Notice to Proceed
---	---	---

Signature over Printed Name

Position/Designation

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 NETWORK MONITORING SYSTEM (SUBSCRIPTION)	
Approved Budget for the Contract (ABC)	Total Offered Quotation
Seven Hundred Fifty Thousand Pesos (Php750,000.00)	In words: _____ _____ _____ _____ In figures: _____ _____ _____ _____

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
NETWORK MONITORING SYSTEM
(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 Seven Hundred Fifty Thousand Pesos (750,000.00), inclusive of all applicable government charges.

II. Technical Specification

1. The Monitoring Solution should provide Unified Architectural design offering seamless common functions including but not limited to:
 - Event and Alarm management,
 - Auto-discovery of the IT environment,
 - Performance and availability management
 - Service Level Management, notifications
 - Reporting and analytics
 - Automation and Customization
2. Should be a tight integration between infrastructure metrics and logs to have the single consolidated console of Infrastructure & security events.
3. Should be able to pull up security events related to a given Configuration Item, from a single console which also has NOC events, and use the security events to triage the problem. This way the Operator gets consolidated system/network event details and security events (current and historical) from the same console and save time in troubleshooting / isolating the issue.
4. Should be able to build correlation rules in a simple GUI based environment where the Operator should be able to correlate cross domain events
5. Shall provide future scalability of the whole system without major architectural changes.
6. Shall be distributed, scalable, and multi-platform and open to third party integration such as Cloud, Virtualization, Database, Web Server, Application Server platforms etc.
7. All the required modules should be from same OEM and should be tightly integrated for single pane of glass view of enterprise monitoring
8. Must provide single integrated dashboard to provide line of business views and drill down capabilities to navigate technical operators right from services to last infrastructure components
9. Consolidated dashboard of the proposed NMS solution must be able to do dynamic service modelling of all business-critical production services & use near-real time Service Model for efficient cross domain event correlation.
10. Must provide SDK/Rest API for North bound and South Bound Integrations e.g. Forwarding specific metric data to third party database, Notifications to third party systems such as Jira, AutoDesk, Slack

Detailed Specifications:

- Must provide complete cross-domain visibility of IT infrastructure issues
- Must consolidate monitoring events from across layers such as Network, Server, Application, Database etc
- Should support single console for automated discovery of enterprise network components e.g. network device, servers, virtualization, cloud, application and databases
- Must support custom dashboards for different role users such as Management, admin and report users
- Must allow creating custom data widget to visualize data with user preferences ex. Refresh time, time span, background color, unit conversion
- Must support multiple visualization methods such as gauge, grid, charts, Top N etc.
- Should provide superior view of infrastructure health across system, networks, application and other IT Infrastructure components into a consolidated, central console
- There should be only one dashboard/interface to collected network/server/application/log data after correlation and consolidation across the IT landscape to reduce/correlate number of metrics/alarms

Network Performance Management

- Shall provide a single integrated solution for comprehensive management of the wired/wireless access, and rich visibility into connectivity and performance assurance issues.
- Shall facilitate creation of templates used for monitoring key network resources, devices, and attributes. Default templates and best practice designs are provided for quick out-of-the- box implementation automating the work required to use OEM validated designs and best practices.
- Must provide comprehensive and integrated management of IT infrastructure components to maximize the availability of IT services and SLA performance.
- Must provide the complete view of the Topology and network elements. The NMS shall have the ability to include the network elements and the links in the visual/graphical map of the department. The visual maps shall display the elements in different color depending upon the status of the element. It is preferable that green color for healthy and amber/yellow color for degraded condition and red for unhealthy condition is used.
- Must have suitable system level backup mechanism for taking backup of NMS data manually as well as automatically
- Must keep historical data at raw level without averaging for minimum of six month
- Must provide the visual presentation of the Network Element's status and the alarms. It shall also present the complete map of the network domain with suitable icons and in suitable color like green for healthy, red for non-operational, yellow for degraded mode of operation etc.

- Must provide Health Monitoring reports of the network with settable periodicity – (24 Hrs, 1 week, 1 month) with no limit of time frame.
- Must provide the graphical layout of the network element with modules drawn using different colors to indicate their status
- Must provide calendar view which allows the operator all the schedule activities such as Reports, Inventory scans etc. It shall also allow to define scheduled report for uptime, link status etc.
- Should have multiple alerting features to get the notification via email, sms and third-party systems
- Must support listening to traps and syslog events from the network devices with no limit on retention period.
- Must support defining the data retention period to control storage
- Must support custom device template to support Generic SNMP devices
- Must provide discovery & inventory of heterogeneous physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices and do mapping of LAN & WAN connectivity with granular visibility up to individual ports level.
- Shall provide Real time network monitoring and Measurement off-end-to-end Network performance & availability to define service levels and further improve upon them.

Fault Management:

- Must provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis. It should also have a strong event correlation engine which can correlate the events on the basis of event pairing, event sequencing etc.
- Must include an event correlation automatically fed with events originating from managed elements, monitoring tools or data sources external to the platform. This correlation must perform:
 - Event filtering
 - Event suppression
 - Event aggregation
 - Event annotation
- Must support creating and monitoring of rising or falling thresholds with respect to basic key performance indicators for network, system and application infrastructures.
- Should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis. It should also have a strong event correlation engine which can correlate the events on the basis of event pairing, event sequencing etc.
- Must have powerful correlation capabilities to reduce number of actionable events. Topology based and event stream-based correlation should be made available.
- Must offer relevant remedy tools, graphs in context of a selected fault alarm/event

- Should have capability to configure actions-based rules for set of pre-defined alarms/alerts enabling automation of set tasks.
- Must support Event or Alarm Correlation integrations with service desk to trigger automated creation of incidents, problems management
- Should classify events based on business impact and also allow defining custom severity levels and priority metrics such as Ok, Critical, Major, Down, Info etc with color codes
- Should allow creation of correlation or analytics rules for administrators
- Must provide default event dashboard to identify, accept and assign generated alarms

Log Management

- Must provide a common classification of event irrespective of the log format
- Must provide the ability to store/ retain both normalized and the original raw format of the event log as for forensic purposes without any time limit and allow to extend it to further with additional hardware without any disruption to the ongoing data collection
- The proposed solution should provide a minimum log compression of 8:1 for ensuring log compression to reduce overall log index storage space for the raw log format
- The log data generated should be stored in a centralized server. The period upto which the data must be available should be customizable.
- Must support logs collected from commercial and proprietary applications. For assets not natively supported, the solution should provide the collection of events through customization of connectors or similar integration
- Must support log collection for Directories (i.e. AD, LDAP), hosted applications such as database, web server, file integrity logs etc. using agents
- The Log receiver or log collection component must store the data locally if communication with centralized collector/receiver is unavailable.
- Must support log collection from Network infrastructure (i.e. switches, routers, etc.). Please describe the level of support for this type of product.
- The system shall support the following log formats for log collection:
 - Windows Event Log
 - Syslog
 - Access Log Data
 - Application Log data
 - Any Custom Log data
 - Text Log (flat file)
 - JSON Data

- Should be able to collect raw logs in real-time to a Central log database from any IP device including:
 - Networking devices(router/switches/voice gateways)
 - Security devices (IDS/IPS, AV, Patch Mgmt., Firewall/DB Security solutions)
 - Operating systems(Windows 2003/2008, Unix, linux, AIX)
 - Virtualization Platforms(Microsoft HyperV, VMware Vcenter/VSphere, 4.X, vDirector, Citrix)
 - Databases(Oracle/SQL/MYSQL/DB2)
- Should support collection of logs through Syslog, syslogNG and also provide native Windows Agents as well as Agentless(PowerShell) connectors
- Must provide alerting based upon established policy
- Must provide SDK and Rest API to write custom connectors and collectors to pull log and monitoring data from third party system
- Must provide UI based wizard and capabilities to minimize false positives and deliver accurate results.
- Must collect, index the log messages and support full-text searching for forensic investigation
- Must support the ability to take action upon receiving an alert. For example, the solution should support the ability to initiate a script or send an email message.
- Must provide pre-defined log correlation rules to detect suspicious behavior
- The solution must support real-time and scheduled alerting time-line while creating a log policy to catch specific log pattern
- Should support applying regex pattern in real-time to extract vendor specific log data for reporting and alerting purpose
- Shall have the capability to drag and drop building of custom search queries & reports
- Shall be capable of operating at a sustained 5000 EPS per collection instance.
- Shall provide the ability to scale to higher event rates by adding multiple collection instance

Role-Based access control

- Should have inbuilt role-based access module to enable multiple users with different groups to create dashboards specific to their department
- Should have way to control and define permission such as read/write for set of devices rather than all the devices for the ease of use.

Other Key Requirements

- Should provide all the modules as a single monitoring engine to correlate events in real-time from Networks, Servers and Applications
- Should be virtual appliance and deployable on Linux operating systems to reduce the overall TCO
- Should have built-in time series database support for better response time, retention and analytics support.
- Should have plugin driven architecture for easy integrations and monitoring of devices.
- Must have bundled annual Branded SMS gateway with 10,000 credits
- Must provide native Windows Agents as well as Agentless (PowerShell) connectors

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 a monthly health check during the subscription period 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. Warranty

The warranty shall be for a period of One (1) year.

V. Others

1. The winning bidder is required to conduct a requirements analysis for the configuration of the whole setup within 15 calendar days after issuance of Notice to Proceed. The bidder must submit complete documentation of the entire work plan, resource (hw/sw) requirements, manpower requirements, network design, course syllabus (for knowledge transfer) etc.
2. 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.

3. At the end of the implementation phase, the winning bidder must submit a comprehensive documentation on the final setup. The documentation should include a network / logical diagram, configuration settings, and all manuals.

VI. Delivery

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

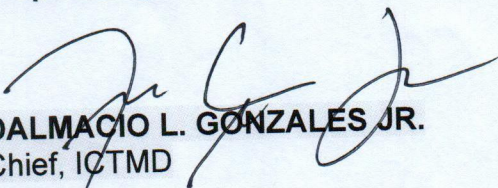
VII. Terms of Subscription

The subscription shall be for a period of One (1) year.

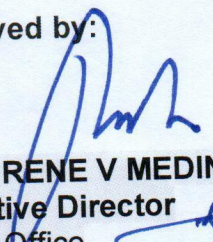
VIII. Payment

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

Division/Section: ICTMD

Date Request: July 14, 2021

PR No. :

2021-07-308

SAI No. :

30 July 2021

Item No.	Unit	Item Description	Quantity	Unit Cost	Total Cost
		SUPPLY, DELIVERY, INSTALLATION AND CONFIGURATION OF NETWORK MONITORING SYSTEM (SUBSCRIPTION)			750,000.00
*****	*****	*****	*****	*****	*****

Requisitioning Officer

Signature:

Printed Name:

VADM RENE V MEDINA AFP (Ret)

Designation

Executive Director
STCW Office

Purpose:

To be used for the management of networking components like routers, switches, firewalls, servers, and VMs are for fault and performance and evaluated continuously to maintain and optimize their availability.

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:

Omnibus Sworn Statement (Revised)

REPUBLIC OF THE PHILIPPINES)
CITY/MUNICIPALITY OF _____) S.S.

AFFIDAVIT

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

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

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

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

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

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

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

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

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

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

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

[If a sole proprietorship:] The owner or sole proprietor is not related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

[If a partnership or cooperative:] None of the officers and members of [Name of Bidder] is related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the

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

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

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

IN WITNESS WHEREOF, I have hereunto set my hand this ___ day of ___, 20__ at _____, Philippines.

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

[Insert signatory's legal capacity]

Affiant

[Jurat]

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