TERMS OF REFERENCE

PROCUREMENT OF PUBLIC CLOUD SERVICES

I. Procurement Objective

The Maritime Industry Authority (MARINA) intends to procure public cloud services from a competent and reputable Cloud Service Provider (CSP) which shall be used for the deployment of other back-end systems of the System Integration Component of the Project.

II. Approved Budget for the Contract (ABC)

MARINA, through the 2023 GAA Fund, intends to apply the sum of **Seven (7) Million Pesos (₱ 7,000,000.00)** being the Approved Budget for the Contract (ABC) to payments under the contract for Procurement of Public Cloud Services. The ABC is the total budget allocated for the duration of the contract which is Twelve (12) months with option to renew, provided the Services rendered are of acceptable quality and cost-beneficial to MARINA, as per Guidelines and Policy of the Government Procurement Policy Board (GPPB) for the Procurement of Water, Electricity, Telecommunications and Internet Service Providers (WETI).

Bids received in excess of the ABC shall be automatically rejected at the opening of the financial proposals.

III. Contract Duration

The initial engagement duration is twelve (12) months upon full activation and acceptance of the Technical Inspection and Acceptance Committee for Information Technology (TIAC-IT) of the procured instances and shall likewise cover the connectivity service, Public IP and Technical Support Services.

IV. Scope of Work

1. The cloud provider will be responsible in provisioning required compute infrastructure (virtual machines/server, storage etc.),
2. The cloud provider should provide support and maintenance which include communication media such as but not limited to telephone, chat, email and remote support.

V. Technical Specifications & Requirements

1. The cloud provider should comply with the following standards:
    a. ISO 9001
    b. ISO 27001
    c. ISO 27017
    d. ISO 27018
    e. SOC1
    f. SOC2

3. The account ownership and its related services shall belong to MARINA. Access rights may be given to third party vendor(s), as deemed necessary, to perform any services related to the project. MARINA however shall have the right and ability to revoke said rights at any given time from the root account.
4. The cloud provider shall provide, as part of the subscribed services, 8x5 Seven Days a week Technical Support to all instances and resources subscribed by MARINA. Support services must include communication mediums such as but not limited to telephone, chat, email, live screen sharing and the likes with response time of at least 2 hours from support ticket logging.
5. The cloud provider shall provide an interactive Graphical User Interface (GUI) with 2-Factor Authentication that allows user to manage all hosting service instantly and securely.
6. The cloud provider must have the capability to deploy a scalable and Multi-AZ. Intent is to prevent single points of failure which may be caused by all forms of natural disasters, outages and other occurrences that may disrupt normal operations.
7. The cloud provider should implement a concept of domains or zones, where multiple data centers are grouped through a low-latency network to provide a higher degree of high-availability and fault tolerance.
8. The cloud provider should have regional presence in the following geographies:
    - North America
    - Europe/Middle East/Africa
    - South America
    - Asia Pacific/South East Asia
9. The cloud provider should have domains or zones with data centers that are located physically apart to support redundancy, high-availability, and low latency.
10. The cloud provider should offer data centers engineered to be isolated from failures in other data centers, with redundant power, cooling, and networking.
11. The cloud provider is capable of offering data replication across data centers within a domain or zone with automatic failover.
12. The cloud provider must have the ability to provide a managed relational database service which can be integrated with any chosen software solutions. This managed relational database will enable the user administrators to optimize time by "outsourcing" the OS patching.
13. The cloud provider must provide a self-service portal which acts as a graphical user interface accessible over the web that will allow cloud administrators and users to conveniently access, provision, modify, and automate subscribed cloud -based resources.
14. The cloud provider must provide a dashboard for cloud administrators which shall provide an overall view of the size and status of the subscribed Cloud Environment.
15. The cloud provider shall provide performance monitoring capabilities for processor, memory, disk usage, and network utilization.
    - 15.1 Provide and actively capture performance-related information of Cloud Environment services or resources.
    - 15.2 Have the ability to send customizable email notifications to administrations based on threshold alarms.
    - 15.3 Have the ability to capture initial performance baseline which can be used to analyze the variation in performance of the services.

15.4 The collected performance metrics or logs shall be made available to the end-user administrator through the self-service portal. The performance metrics shall be presented in a unified manner with appropriate visualization.

16. Isolated Private Network and Private Cloud Options:

16.1 All cloud instances and services must be hosted within an isolated private network or virtual private cloud that can support up to 600GB per month data transfer out from the cloud.

16.2 The cloud provider must have the ability/option to provide dedicated virtual machines and hosts should MARINA decides the need for it.

16.3 Must be able to support IPv6 Protocol.

17. The cloud provider must be able to engage in an On-Demand or Pay-per-Use Model where MARINA will pay based on usage and not based on reserved instances.

18. Data Sovereignty

18.1 MARINA subject to conditions prescribed by the Law of the Republic of the Philippines with regards to data residency and sovereignty laws, retains control and ownership of all data stored or processed during the subscription period.

18.2 All MARINA Data stored in the Cloud shall be the sole property of MARINA. This data can be retrieved anytime upon request of MARINA and has the sole right and authority to copy, move, delete, or transfer it to other locations.

18.3 The cloud provider must agree and ensure that the data stored in an agreed location will remain within it and will not be transferred without the knowledge of MARINA.

19. MARINA requires the cloud provider as a recognized "Leader" in Gartner's Infrastructure-as-a Service (IaaS) Magic Quadrant for at least three (3) consecutive years and is still recognized as a "Leader" at the same year of MARINA's procurement of the said service.

20. Compute and Storage Sizing Requirements

20.1 MARINA shall engage the cloud provider on an On-Demand or Pay-per-Use model. As such, the sizing requirements stated herein shall be the initial set of resources to be subscribed by MARINA.

20.2 The initial sizing required is tabulated below:

Item	Server Name	Description/ Application	Instance Type	EBS Volume	OS
Managed Server	API 1	PHP/LARAVEL	vCPU-4 Mem - 16GiB	200 GIG	LINUX AMI 2 or Equivalent
Managed Server	API 2	PHP/LARAVEL	vCPU-4 Mem - 16GiB	200 GIG	LINUX AMI 2 or Equivalent
Managed Server	API 3	PHP/LARAVEL	vCPU-4 Mem - 16GiB	201 GIG	LINUX AMI 2 or Equivalent
Managed Server	API 4	PHP/LARAVEL	vCPU-4 Mem - 16GiB	202 GIG	LINUX AMI 2 or Equivalent
Managed Server	API 5	PHP/LARAVEL	vCPU-4 Mem - 16GiB	203 GIG	LINUX AMI 2 or Equivalent
Managed Server	API 6	PHP/LARAVEL	vCPU-4 Mem - 16GiB	204 GIG	LINUX AMI 2 or Equivalent
Managed Server	API 7	PHP/LARAVEL	vCPU-4 Mem - 16GiB	205 GIG	LINUX AMI 2 or Equivalent
Managed Server	FE SITE	REACTJS	vCPU-2 Mem - 8GiB	206 GIG	LINUX AMI 2 or Equivalent
Managed Server	FE SITE	REACTJS	vCPU-2 Mem - 8GiB	207 GIG	LINUX AMI 2 or Equivalent

Managed Server	FE CORE	REACTJS	vCPU-2 Mem - 8GiB	208 GIG	LINUX AMI 2 or Equivalent
Managed Server	FE CORE	REACTJS	vCPU-2 Mem - 8GiB	209 GIG	LINUX AMI 2 or Equivalent
Managed Data-base	DATA BASE	MYSQL	vCPU-4 Mem - 32GiB	1TB	N/A
Managed Server	ELASTIC SEARCH	ELASTIC SEARCH	vCPU-2 Mem - 8GiB	500 GIG	LINUX AMI 2 or Equivalent
Managed Server	Bastion Server	Bastion Server	vCPU-2 Mem - 4GiB	100GB	Windows

20.3 Infrastructure Security Requirements

20.3.1 Web Application Firewall (WAF)

20.3.1.1 Requires web application protection from attacks by enabling configure rules that will allow, block, or monitor and quantify web requests based on defined conditions. These conditions include IP addresses, HTTP headers, HTTP body, URI strings, SQL injection and cross-site scripting.

20.3.1.2 Must protect websites from common attack techniques like SQL injection and Cross-Site Scripting (XSS).

20.3.2 File System Storage

20.3.2.1 A fully managed service that provides cost-effective, high-, performance scalable storage for compute workloads.

20.3.2.2 Offers sub-millisecond latencies, up to hundreds of gigabytes per second of throughput, and millions of IOPS.

20.3.2.3 Capable of accessing and processing data concurrently from both a high-performance file system and from the API.

20.3.3 Cloud Distributed Denial of Service (DDoS) Protection

20.3.3.1 Must provide fast, reliable and efficient Content Delivery Network (CDN) service that securely delivers data, applications, and APIs with low latency and high transfer speeds, providing an additional layer of protection from DDoS attacks.

20.3.3.2 Must provide an always-on detection and automatic inline DDoS mitigations that will mitigate or minimize application downtime and latency.

20.3.3.3 Provides 24x7 access to the cloud providers and protection against DDoS related spikes in cloud instances/VMs, load balancers, content delivery network (CDN), and DNS changes.

20.3.4 Secured Monitoring

20.3.4.1 Must support metric alarm, data collection and tracking on cloud resources.

20.3.4.2 Must support access through APIs, Command Line Interface (CLI), programming software development kits (SDKs), and the Cloud Provider management console.

20.3.4.3 Able to provide metric alarms and interactive analytics capability for metric logs.

20.3.4.4 Must be able to create metric dashboards.

20.3.5 Virtual Private Network (VPN)

20.3.5.1 Supports Site-to-Site VPN for secure connectivity from on-premise to the off-shore Cloud Infrastructure.

20.3.5.2 Site-to-Site VPN must support statically routed or dynamically routed VPN connections.

20.3.5.3 Each Site-to-site VPN must support two tunnels, with each tunnel supporting maximum of 1.25Gbps bandwidth.

21. Data Sovereignty, Data Residency and Data Privacy Compliances

21.1 The cloud provider is required to comply with Data Sovereignty Guidelines and Policies as prescribed in the Philippine Government's Cloud First Policy:

21.1.1 All data created, collected, organized, modified, retrieved, used, consolidated, sourced from, or owned by the Philippine Government, including all its agencies and instrumentalities, or by any national of the Philippines or any entity that has links to the Philippines, which are in the cloud, regardless of location, shall be governed by Philippine Laws, policies, rules and regulations.

21.1.2 Except as otherwise permitted under Philippine Law, no such data shall be subject to foreign laws, or be accessible to other countries, regardless of the cloud deployment model used, the nationality of the cloud provider, or the data's place of storage, processing, or transmission. No right appurtenant to such data shall be deemed transferred or assigned by virtue of the storage, processing, or transmission thereof by the cloud provider.

21.1.3 The cloud provider and other entities engaged in the storage, processing, or transmission of such data shall comply with all applicable Philippine Laws, policies, rules, regulations and issuances relating to data sovereignty, and confidentiality, inclusive of RA 10844, RA 10173, RA 10175, their implementing rules and regulations.

21.2. The cloud provider shall adhere to the Philippine Cloud First Policy on Data Residency, specifically for the handling of **Sensitive Government Data** as defined in Section 12.2., item "a" of the Department of Information and Communications Technology (DICT) Department Circular No. 010, more specifically known as the Amendments to the Prescribed Philippine Government's Cloud First Policy.

As a general rule, no residency restrictions shall be placed on government data stored or processed in the cloud, provided that appropriate controls and security measures are present. By way of exception, the storage or processing of sensitive government data shall be restricted to the following:

21.2.1. The Philippine Territory.

21.2.2. Other territories over which the Philippines exercises sovereignty or jurisdiction.

21.2.3. Other countries or states with which the Philippines has enforceable extradition treaties for the turnover of persons accused or convicted of violating Philippine laws, provided such other countries or states shall:

21.2.3.1. Similar or higher standards of protection or Philippine Government data as Philippine Laws and issuances; or

21.2.3.2. Existing agreements with the Philippine government for the provision of similar or higher protection to Philippine government data as Philippine Laws and Issuances.

21.3. The cloud provider shall abide by Republic Act (RA) 10173, otherwise known as the Data Privacy Act of 2012.

22. Service Level Agreement(SLA)

Cloud Service Level commitment with a Monthly Uptime Percentage of 99.99%. In the event any of the Subscribed Services are not able to meet the Service Level Commitment, MARINA will be eligible to receive a Service Credit as described below:

Monthly Uptime Percentage	Service Credit Percentage
Less than 99.99% but equal to or greater than 99.0%	10%
Less than 99.0% but equal to or greater than 95.0%	25%
Less than 95.0%	100%

22.1. The Bidder shall provide a basic support plan that will deliver the following:

22.1.1. 8 x 5phone, email, and chat access to Cloud Support Engineers

22.1.2. Should have the following support:

- Support Helpdesk
- Email Support
- Remote Support

22.1.3. Service Level Defined

Severity Level	Severity Description
1 = Critical	Service connection is unavailable and downtime impacts business operations; show stopper. A critical problem in the infrastructure which may severely impact the client'soperations, or in which client's production systems are down or not functioning; loss of production data and no procedural work around exists.
2 = High	A problem where the infrastructure is available and intermittent accessibility. That requires immediate infrastructure assessment and evaluation. The situation is causingsignificant impact to portions of the client's business operations and productivity. The system is exposed to potential loss or interruption of service.
3 = Medium	Change management process on infrastructure specifications upgrade, additional relates services which requires scheduled downtime and Reboot. Medium to Low impact. which involves partial non-critical functionality loss. One which impairs some operations but allows the client to continue to function. This may be a minorissue with limited loss or no loss of functionality or impact to the client's operation and issues in which there is an easy avoidance by the end user
4 = Normal	Minimal downtime, required for reboot, patches, and updates. Minimal business operationimpact.
5 = Low	A general usage questions or recommendation for a future enhancement or modification.Concerns are answerable by FAQ or by email or phone within the same day. There is no impact on the quality, performance or functionality of the infrastructure

22.2. Response Time

Severity Level	Response Time	Resolution Time	Frequencyof UpdateStatus on Resolution
Severity 1	Phone: Immediate Mail: Within 15 Mins	Infrastructure and application to be restoredwithin 5 hours from response sent to client.	Every 30 minutes
Severity 2	Email/phone: Within 30 Mins	Infrastructure and application to be restoredwithin 8 hours from response sent to client.	Every hour
Severity 3	Email/phone/remote: Within 1 hour	Within 12 hours	One time

Severity 4	Email/phone/remote: Within 2 hours	Within 24 hours	One time
Severity 5	Email/phone: Within 2 hours	Within 24 hours	One time

23. Support Service

Infrastructure Managed Services Coverage

- **Technical support and services**
- **Proactive Infrastructure monitoring:**
  - ✓ Preventive systems down
  - ✓ Virtual Servers and DB
  - ✓ 8x5 Seven Days a week monitoring level
- **Pro-active System Health checks quarterly**
- **Server maintenance and performance monitoring**
  - ✓ CPU usage
  - ✓ Bandwidth usage
  - ✓ Memory usage
  - ✓ Storage usage
- **Capacity monitoring**
  - ✓ Quarterly Report of total bandwidth usage
  - ✓ Quarterly Report of threshold crossing incidents
  - ✓ Quarterly Report pertaining to capacity
- **Security patches and updates**

24. Cloud Administration Services

24.1. Implementation services for all cloud components proposed by the bidder.

24.2. Administer key aspects of MARINA cloud infrastructure including the underlying compute and storage components. The bidder will manage users, directories, access rights, disk space, and processes.

24.3. The bidder will monitor system and resource alerts, resource utilization and resource contention to support the environment.

24.4. The bidder will utilize existing cloud tools to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in MARINA's cloud resources.

24.5. As part of the service improvement plan, the bidder will provide MARINA recommendations on cost optimization.

24.6. The bidder will administer the deployed security controls to manage the user access using Identity and Access Management tools

25. Cloud Infrastructure Training

25.1 The bidder will provide end-user training.

25.2 The trainings shall provide the option for virtual or live classes.

VI. PROJECT SCHEDULE

Description	Activities / Deliverables	Timelines
Project Kick-off	• Data gathering and assessment	• Ten (10) Calendar Days Upon Receipt of Notice to Proceed
	• Submission of the following: - Final detailed Project Plan - Final detailed work plan - Roles and Responsibilities Definition	• Five (5) Calendar Days after the Project Kickoff
Project Implementation	• Installation, Setup and Configuration of Cloud Infra, Security tools • Server Hardening	• Thirty (30) Calendar Days after the Project Kickoff
Migration	• Server Migration : 11 API Servers and 1 DB Server	
Go Live	• Go live (Cloud Infra, Security Tools)	
Stabilization and Monitoring	• Monitoring and Issue Resolution	
Turnover / Documentation and Project Closure	• Implementation reports and documentation • Knowledge Transfer • User Acceptance / Sign Off	

VII. INSTALLATION AND CONFIGURATION

a. The Project Kickoff and submission of Project Plan and Detailed Work Plan must be conducted within 15 Calendar Days upon receipt of Notice to Proceed.
b. The project must be completed within Thirty (30) Calendar Days after the Project Kickoff.

VIII. QUALIFICATION OF THE BIDDER

a. The bidder should have at least seven (7) years of operation in the IT Industry with proven track experience in IT Security, Development, Consultancy, Training and Professional Services.
b. The bidder shall submit a proof of valid ISO Certification for the product as follows: ISO 9001, ISO 27001, ISO 27017, ISO 27018, SOC1, and SOC2 The bidder shall submit proof that they are a Cloud Consulting Partner and Solution Provider Program Partner of the product being offered.
c. The bidder must have atleast (5) cloud implementation project, for both Commercial and Public Sectors within the last 2 years, The project must atleast two (2) million each.

IX. PAYMENT

MARINA shall pay its subscription on a monthly basis.

a. The accumulated payables within the validity of the Subscription Period must not exceed the ABC set for this procurement.
b. All activated additional resources must be billed separately.
c. All chargeable costs must be inclusive of VAT.

Prepared by:

DALMACIO L. GONZALES JR.
Chief, ICTMD

Recommending Approval:

SAMUEL L. BATALLA
Officer-In-Charge
Office of the Executive Director
STCW Office

Reviewed by:

ATTY. BENEDICTO G. MANLAPAZ
Head, TWG for IT

DIR. ARSENIO F. LINGAD II
Chairperson, MARINA BAC

APPROVED / ~~DISAPPROVED~~:

Atty. HERNANI N. FABIA
Administrator

Version 1 – October 5, 2022