ASD NO.: 13-00
Initial Issue Date: 09-08-2017
Revision Date: 00

REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF TRANSPORTATION
MARITIME INDUSTRY AUTHORITY

PURCHASE REQUEST

Office: STCW OFFICE
Division/Section: ICTMD
Date Request: February 27, 2019

PR No. : 2019-03-37 STCW'd
SAI No. : MAR 0 5 2019

Item No.	Unit	Item Description	Quantity	Unit Cost	Total Cost
		LEASED OF REPLICATION SERVICES (CLOUD-BASED BACKUP AND RECOVERY SOLUTION)			**800,000.00**
		x-x-x-x-x-x-x			

NOT INCLUDED IN THE APP for FY 2019
CONSUELO T. DELA CRUZ
GSD-Procurement Section

Requisitioning Officer

Signature:	
Printed Name:	**ATTY. VERA JOY S. BAN-EG**
Designation	Deputy Executive Director, STCW Office

Purpose:

For the use of MARINA Integrated Seafarer's Management Online (MISMO) System

CERTIFICATION

☑ FUNDS AVAILABLE
☐ NO FUNDS AVAILABLE

RALPH A. NARVAEZ
OIC, Budget Division

☐ Approved ☐ Disapproved

PR Approver

Signature:	
Printed Name:	**VADM NARCISO A VINGSON JR**
Designation	OIC, Administrator

Note:

www.marina.gov.ph

TERMS OF REFERENCE

PROCUREMENT OF CLOUD-BASED BACKUP AND RECOVERY SOLUTION

I. INTRODUCTION

The Maritime Industry Authority (MARINA) was created on 01 June 1974 as an attached Agency to the Office of the President (OP). With the issuance of Presidential Decree No. 474, otherwise known as the "Maritime Industry Decree of 1974", to integrate the development, promotion and regulation of the maritime industry in the country and the creation of the Ministry (now Department) of Transportation (DOTr) by virtue of Executive Order No. 546, the MARINA was attached to the DOTr for policy and program coordination on 23 July 1979.

One of the major requirements of the MARINA Online processing is the availability of internet facility that has efficient capability to access electronic data and information from different sources and share electronic data and information.

III. OBJECTIVE

To provide cloud-based backup and recovery solution from March to December 2019.

IV. PROCUREMENT STRATEGY

Acquisition shall be done through the most appropriate procurement process as defined in RA 9184 and shall be covered by separate contracts.

V. EXPERTISE AND QUALIFICATIONS

The bidder must have the following expertise and experience in providing the necessary services required by MARINA;

a. At least two (2) years expertise and experience in Back Up Cloud Service;
b. Ability to provide maintenance services and technical support;
c. Bidder should submit a letter of support from the principal cloud service provider as part of the bid/proposal.

VI. TECHNICAL SPECIFICATIONS

Solution Architecture

a. The solution must utilize cloud-based components as the primary site for availability and scalability.
b. The solution must use multiple availability zones for high availability for the different application layers.
c. The solution must utilize NAT gateways for internet traffic.
d. The solution should have the capability to scale up when needed to cater for increase in workloads.
e. The solution must use load balancers across availability zones for workload distribution.
f. The solution must utilize a fully-managed, open source relational database management system (RDBMS).
g. The RDBMS must utilize a high performance storage subsystem
h. The RDBMS must utilize a virtual database storage volume that spans multiple availability zones, with each availability zone having a copy of the RDBMS cluster data.
i. The RDBMS must utilize cloud object storage for backup via snapshots.
j. The solution must utilize host and subnet security controls for incoming and outgoing data filtering via IP addresses and port numbers.
k. The solution must replicate data from the cloud RDBMS to the on-premises RDBMS.
l. The solution must use a cloud service to perform replication of the RDBMS to the on-premises data center for disaster recovery.
m. The solution must provide for a stand-by server for the application server for disaster recovery. (Server to be provided by MARINA)
n. The solution must provide for a stand-by server for the database server for disaster recovery. (Server to be provided by MARINA)
o. The solution must provide for a secure Virtual Private Network (VPN) connection from the on-premises network to the virtual private cloud network. (On-premises VPN server to be provided by MARINA)
p. The solution must utilize a cloud-based object storage back-end as a file server.
q. The solution must utilize a cloud-based, fully managed search database engine

r. The Site/Admin application layer must have at least one(1) vCPU and two (2) GiB of memory in a load balanced, highly available configuration.
s. The API application layer must have at least four (4) vCPU and sixteen (16) GiB of memory in a load balanced, highly available configuration.
t. The search engine component must have at least one (1) vCPU and two (2) GiB of memory.
u. The RDBMS component must have at least two (2) vCPU and fifteen (15) GiB of memory.
v. The file server component must have at least two (2) vCPU and four (4) GiB of memory.
w. The replication server component must have at least two (2) vCPU and four (4) GiB of memory.

Cloud Provider Infrastructure Capabilities

a. The cloud provider should have at least ten (10) years of operation in the public cloud market.
b. 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.
c. The cloud provider should have regional presence in the following geographies:
    - North America
    - Europe/Middle East/Africa
    - South America
    - Asia Pacific
d. The cloud provider should have domains or zones with data centers that are located physically apart to support redundancy, high-availability, and low latency.
e. The cloud provider should offer data centers engineered to be isolated from failures in other data centers, with redundant power, cooling, and networking.
f. The cloud provider is capable of offering data replication across data centers within a domain or zone with automatic failover.

Cloud Compute Instance Capabilities

a. The cloud provider should offer the following instance types:
    - General Purpose
    - Memory Optimized
    - Compute Optimized
    - Storage Optimized
    - Graphics Optimized
    - FPGA Optimized
    - Burstable Instances
    - I/O Intensive Instances
b. The cloud instance should support multiple (primary and additional) network interface cards (NICs).
c. The cloud provider should offer users the capability to logically group instances together within the same data center.
d. The cloud provider should offer self-service provisioning of multiple instances concurrently either through a programmatic interface, a management console, or a web portal.
e. The cloud provider should provide for the capability of single tenant instances that run on hardware dedicated to a single user.
f. The cloud provider should offer the ability to launch an instance and specify that this instance always restarts on the same physical host.
g. The cloud provider should offer the ability to automatically increase the number of instances during demand spikes to maintain performance (i.e. 'scale-out').

Cloud Networking Capabilities

a. The cloud provider should support the ability to create a logical, isolated virtual network that represents an agency's own network in the cloud.
b. The cloud provider offer the capability of creating fully isolated (private) virtual networks and subnets where instances can be provisioned without any public Internet protocol (IP) address or internet routing.

c. The cloud provider should support Internet protocol (IP) address ranges specified in the request for comments (RFC) 1918 as well as publicly routable classless inter-domain routing (CIDR) blocks.
d. The cloud provider should support multiple protocols including transmission control protocol (TCP), user datagram protocol (UDP), and Internet control message protocol (ICMP).
e. The cloud provider should support Internet protocol (IP) addresses associated with a user account, not a particular instance. The IP address should remain associated with the account until released explicitly.
f. The cloud provider should support the ability to assign a primary and a secondary Internet protocol (IP) address to a network interface card (NIC) that is attached to a given instance.
g. The cloud provider should support the ability to move network interface cards (NICs) as well as Internet protocol (IP) addresses between instances.
h. The cloud provider should offer the capability of capturing network traffic flow logs.
i. The cloud provider should provide a network address translation (NAT) gateway managed service to enable instances in a private network to connect to the internet or other cloud services, but prevent the Internet from initiating a connection to those instances.
j. The cloud provider should have the ability to disable source/destination check on network interface cards (NICs).
k. The cloud provider should support virtual private network (VPN) connectivity between the cloud provider and the user's data center.
l. The cloud provider should support multiple virtual private network (VPN) connections per virtual network.
m. The cloud provider should allow users to access cloud services via either an Internet protocol security (IPsec) virtual private network (VPN) tunnel or secure sockets layer (SSL) virtual private network (VPN) tunnel over the public Internet.
n. The cloud provider should offer a front-end (Internet-facing) load balancing service that takes requests from clients over the Internet and distributes these requests across instances that are registered with the load balancer.

o. The cloud provider should offer a back-end (private) load balancing service that routes traffic to instances hosted in private subnets.
p. The cloud provider should provide logs that capture detailed information about all requests sent to a load balancer.

Cloud Storage Capabilities

a. The cloud provider should offer block level storage volumes to use with compute instances.
b. The cloud provider should support solid state drive (SSD) backed storage media that offers single digit millisecond latencies.
c. The cloud provider should offer users the ability to increase the size of an existing block storage volume without having to provision a new volume and copy/move the data.
d. The cloud provider should have snapshot capability for its block storage service.
e. The cloud provider should offer server-side encryption of data at-rest for data stored on volumes and its snapshots.
f. The cloud provider offer secure, durable, highly-scalable object storage for storing and retrieving any amount of data from the web.
g. The cloud provider should offer object storage tiering capability, i.e. the ability to recommend transitioning an object between object storage classes or tiers based on its frequency of access.
h. The cloud provider should support managing an object's lifecycle by using a lifecycle configuration, which defines how objects are managed during their lifetime, from creation to deletion.
i. The cloud provider should support server-side encryption (SSE) of data at-rest, with the cloud provider managing the encryption keys in object stores.
j. The cloud provider should allow a user to mark an item as undeletable in object stores.
k. The cloud provider should support multi-factor authentication (MFA) for delete operations as an additional security option in object stores.

Cloud Administration Capabilities

a. The cloud provider should offer a service to create and manage users and groups of users of its infrastructure and its resources.
b. The cloud provider should allow users to reset their own password in a self-service manner.
c. The cloud provider should offer the ability to add permissions to users and groups at the resource-level.
d. The cloud provider infrastructure should contain built-in access control policies that can be attached to users and groups.
e. The cloud provider should offer a mechanism to test the effects of access control policies before committing such policies into production.

Cloud Security

a. The cloud provider should offer a service to protect from common, most frequently occurring network and transport layer distributed denial of service (DDoS) attacks.
b. The cloud provider should comply with the following standards:
    - ISO 9001
    - ISO 27001
    - ISO 27017
    - ISO 27018
    - SOC1
    - SOC2

CLOUD INFRASTRUCTURE SETUP AND CONFIGURATION SCOPE OF WORK
SLA and Managed Services

SUMMARY of Professional Services (SOW)

I. Project kick-Off
II. Project Overview
III. Architecture Jumpstart
IV. Project Assessment
V. Preparation Phase
VI. Landing Zone Design
VII. Approval
VIII. Landing Zone Build
IX. User Acceptance

I. Project kick-Off

a. Project Review of Cloud WEB application Infrastructure and DR prerequisite for MARINA

   i. Applications
   ii. Database
   iii. Storage
   iv. DR type
   v. Network etc.
   vi. Project Team /Role and responsibilities
   vii. Service Provider to provide resource team during the preplanning
      1. DevOps Cloud Engineer
      2. Project manager
      3. Solutions Architect

b. Application Discovery is collecting of usage and configuration data about the proposed project. This will review and discover the Operating System, static configuration, data, utilization, metrics, performance information, Network inbound/outbound connections and running processes.

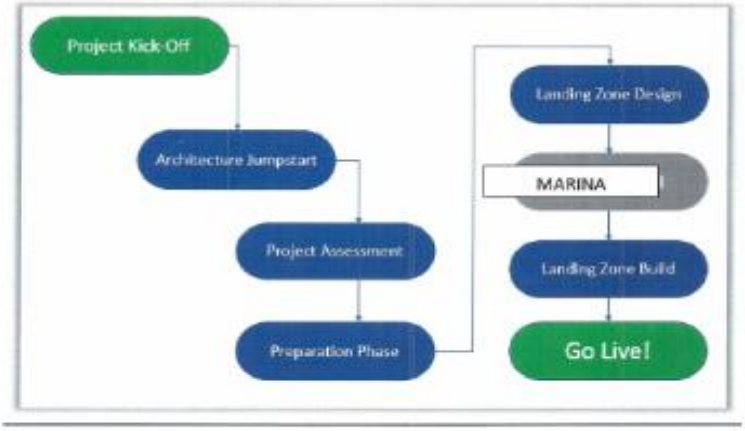
c. Network Discovery is a collecting of any integration of the proposed project to any third-party application.

d. Pre-requisites and Checklist need to define before the start of the proposed project. Define what are the show stopper that can hinder the development of proposed project.

e. Storage for Back up and DR

f. Others tools needed during the Implementation

Project Overview



II. **Architecture Jumpstart**

a. Verification of Gathered Data from Application Discovery and Network Discovery
b. Selection
c. Analysis
d. Architecture Design
e. Functional Cloud to be implemented
f. Account Discussions
g. Others

III. **Project Assessment Review and approval**

a. Project Plan
b. WBS,
c. RACI
d. Implementation timeline

IV. Project Preparation Phase

a. All sources should be listed and prepared from Manpower (AppDev), Application, OS, Server, Platform, Programming language, Database back up and or 3rd party tools.

V. Landing Zone Design and set-up

a. AWS Infrastructure setup
b. AWS Account setup under AWS Organization (Account Management, Production, Staging Development, network, back-up etc)
c. Create Cross Account Access with IAM
d. Create VPC for Production, Staging and Development Environment
e. Creation of Subnets Per VPC
f. Creation of VPC Peering for Production, Staging and Aws Environment
g. Identify security services needed for the implementation

VI. MARINA Approval of AWS Landing Zone

a. Application test , back-up;

VII. BUILD and Implement

a. Back-up plan and procedures

VIII. Implement Other tools and component

IX. Review and other revisions change management request if any

X. Final Documentation, submission of template, configuration, User account, change access password, removal of test environment etc.
a. Security hardening

XI. Go Live Launching of AWS Infrastructure

XII. End-user Acceptance

Service Provider Roles and Responsibilities

Service Provider has the following general responsibilities under Managed Services

- Service Provider will conduct business in a courteous and professional manner with the Customer.
- Service Provider will log all information obtained from the MARINA that is required to establish a Support Request, including the severity level, date of request, problem and current situation of the AWS Infrastructure and application.
- Once a Support Request has been submitted, Service Provider has the responsibility to follow proper tagging of severity level and resolution time needed to complete it.
- For Severity Level 1 and 2, Service Provider will attempt to resolve problems presented over the phone on the first call when received from MARINA.
- The Service Provider will notify Customer upon completion of a Support Request.
- The Service Provider has the responsibility to assign a dedicated Technical Support to client during and after the implementation
  - Pre Implementation
  - DevOps Cloud Engineer
  - Project Manager
  - Solutions Architect
  - Post Support
    - Devops

X. TERMS OF PAYMENTS

Payment shall be made on monthly basis for subject to submission of billing statement and other supporting documents by the winning and the issuance of certificate of satisfactory service by the MARINA.

XI. APPLICABILITY

This Terms of Reference shall form part of the contract documents pertaining to the procurement of Cloud-Based backup and Recovery Solution.

XII. APPROVED BUDGET FOR THE CONTRACT(ABC)

The Approved Budget for the Contract (ABC) inclusive of administrative fees, VAT and all government taxes is Eight Hundred Thousand Pesos **(P 800,000.00)**.