Terms of Reference
CLOUD PLATFORM FOR OSG

A. CLOUD REQUIREMENTS

Rationale

In compliance with the Government's "Cloud First Policy" mandate, the Office of the Solicitor General is planning to use cloud computing to enable ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

This is in adherence to the requirement to partially replace the antiquated server and backup infrastructure of OSG. This cloud migration will help the agency reduce ICT acquisition and operation costs, achieve operational excellence, reduce security gaps, increase employee productivity, and develop excellent online services.

The Renewal of Cloud Computing Services subscription period shall be twelve (12) months from May 31, 2023.

The subscription to cloud computing services will maintain the performance and functionality of its systems and ensure its compatibility with the existing setup of OSG application systems and databases. Hence, reference to brand names is authorized under Section 18 of 2016 Revised IRR of RA 9184, which provides that "reference to brand names shall not be allowed except for items or parts that are compatible with the existing fleet of equipment of the same make and brand, and to maintain the performance, functionality and useful life of the equipment." (Emphasis supplied)

1. AVAILABILITY

The online subscription to the cloud computing platform shall be made available 24/7 to the authorized users of the OSG throughout the entire duration of the 1-yr subscription.

2. SCOPE OF SERVICES

The web hosting service and standard web hosting support service provider shall:

- Supply and deliver the required services stipulated in the Purchase Request

- The cloud service provider, through its local counterpart technical support, will be responsible for provisioning the required cloud platform, services, and associated licenses with the following specifications to ensure compatibility with OSG continuous services follow:

Service Features	Requirements	Compliance
Traffic Management	Capability to control the distribution of traffic across application endpoint. Continuous monitoring of endpoint health and status	
IP Requirement	Provide public IP resources to communicate with other cloud resources, on-premises networks, and the internet	
Security	Inclusion of a unified security management platform that includes security health monitoring of cloud workloads, and security threat blocking through access and application control	
Privacy	Must adhere to the Data Privacy Act of 2012 (RA 10173), must offer continuous security health monitoring for the entire cloud environment	
Scalable Resources	Provide the capability to increase/decrease resources as needed to support any periods of unpredictable resource usage. Scalable resources must include Bandwidth, Servers, Storage, and Database instances	
Vendor Support	Virtual machine availability and connectivity must be at least 99% up all the time	

3. MINIMUM REQUIRED SPECIFICATIONS / FEATURES

DESCRIPTION	Statement of Compliance
GENERAL REQUIREMENTS	
1. Hosting the cloud-based systems developed and implemented by the OSG.	
2. Fully compatible and integrated with the existing cloud-hosting platform of OSG.	
3. Fully compatible to integrate with OSG's existing on-premises environment.	
4. First-party single sign-on capability with OSG's identity and access management service	
5. The proposed cloud solution must be in the "leader's quadrant" in Infrastructure Services in the Gartner Magic Quadrant 2021	
6. The solution must be in an Infrastructure-as-a-Service environment and Platform-as-a-Service Environment	
7. Continuously use the existing OSG tenant account	
8. The solution must support Platform as a Service – it provides a platform allowing one to develop, run and manage applications without the complexity of building and maintaining the infrastructure.	
9. The solution should enable seamless resource/workload movement from cloud source to destination.	
10. The cloud service provider offers better security for applications and data than the security would attain in-house.	
11. The solution must have an IaaS that provides all the infrastructure to support web apps, including storage, web and application servers, and networking resources.	
12. The solution must have a framework for easily building and customizing cloud-based applications	

13. The solution must support geographically distributed development teams	
14. The solution must efficiently manage the application lifecycle	
15. The solution must have an IaaS that makes it quick and economical to scale dev/test environments up and down.	
16. The solution must simplify the planning and management of backup and recovery systems.	
17. The solution must have a Web Application Firewall (WAF).	
18. The solution must have a Managed DNS.	
19. The solution must have a Managed SQL database in the cloud.	
20. The solution must have Microsoft Defender for the cloud	
21. All data at rest and in transit must be encrypted.	
22. The solution must have a DevOps tool	
23. The solution must have equivalent server specifications based on the existing solution.	
24. The solution must retain the current fully qualified domain name	
25. The solution must be capable and compatible with hosting the existing cloud environment	
26. The cloud SQL database must be accessible anywhere to update the table contents but must have proper security measures.	
27. The solution must have an interactive Graphical User Interface (GUI) accessible in any location, allowing the cloud administrators and development teams to conveniently access, manage, provision, and modify all cloud services and components instantly and securely. Multi-factor Authentication is recommended.	

28. The solution must have monitoring tool/s for application performance, analytics, system health, and diagnostic logs.	
29. The winning bidder must provide As-Built documentation or manual, including testing results.	
30. The winning bidder will be responsible for migrating instances and workloads from MS Azure to another provider if the present platform or provider differs from the hosted solution.	
SECURITY REQUIREMENTS	
1. Security has the feature of continually assessing the security posture, tracking new security opportunities, and precisely reporting progress.	
2. Security can secure the workloads with step-by-step actions that protect the workloads from known security risks.	
3. Security can generate a secure score for your subscriptions based on an assessment of your connected resources	
4. Security can detect threats targeting Azure services, including Azure App Service, Azure SQL, Azure Storage Account, and more data services.	
5. security can defend the workloads in real-time so can react immediately and prevent security events from developing.	
6. The security has advanced threat protection features for virtual machines, SQL databases, containers, web applications, your network, and more	
7. security can help limit exposure to brute force attacks.	
8. The security has capabilities that help automatically classify data in Azure SQL.	
WEB APPLICATION FIREWALL	
1. Must have protection against web vulnerabilities and attacks.	

2. Must be capable of protecting multiple websites or applications.	
3. WAF Policies must be customizable for each web application.	
4. Protection against malicious bots and IPs.	
5. Must have protection against common attacks such as SQL Injection, cross-site scripting, command injection, HTTP hi-jacking, HTTP protocol violation and anomalies, crawlers, and scanners.	
6. Must have geo-location filtering.	
7. Must be capable of inspecting JSON and XML.	
8. Must be integrated and configured with the centralized monitoring tool for centralized monitoring.	
9. Must have customizable rules/policies to suit application requirements	
10. Must have logging and monitoring that can be saved or imported to PDF for printing.	
11. Must be integrated and configured with the centralized monitoring tool.	
INFRASTRUCTURE	
1. Must have a financially backed service level agreement (SLA) that guarantees monthly availability.	
2. Must provide preferential discounts for Virtual Machine services for securing longer term consumption and Bring Your Own License (BYOL) with corresponding software maintenance program.	
3. Must provide extended security updates for Windows Server 2008 and SQL Server 2008 workloads moving to the cloud without additional cost.	

4. Must provide additional 3-year extended security updates for Windows Server 2012 and SQL Server 2012 workloads moving to the cloud with additional cost.	

4. Cloud Resources

- **Bill of Materials**

Service type	Custom Name	Region	Description
Application Gateway		Southeast Asia	Web Application Firewall V2 tier, 734 Fixed gateway Hours, 5 GB Data transfer
App Service		Southeast Asia	Free Tier; 1 F1 (0 Core(s), 1 GB RAM, 1 GB Storage) x 730 Hours; Linux OS
App Service		Southeast Asia	Premium V2 Tier; 1 P1V2 (1 Core(s), 3.5 GB RAM, 250 GB Storage) x 730 Hours; Linux OS; 0 SNI SSL Connections; 0 IP SSL Connections
App Service		Southeast Asia	Standard Tier; 1 S1 (1 Core(s), 1.75 GB RAM, 50 GB Storage) x 730 Hours; Linux OS; 0 SNI SSL Connections; 0 IP SSL Connections
Database for MySQL		Southeast Asia	Flexible Server Deployment, Burstable Tier, 1 B1s (1 vCores) x 730 Hours, 20 GB Storage with LRS redundancy, 0 Additional IOPS, 0 GB Additional Backup storage with LRS
Database for MySQL		Southeast Asia	Single Server Deployment, General Purpose Tier, 1 Gen 5 (2 vCore) x 730 Hours, 50 GB Storage with ZRS redundancy, 0 GB Additional Backup storage - LRS redundancy
DNS			Zone 1, DNS, Private; 2 hosted DNS zones, 0 DNS queries

Front Door			Front Door Standard - Base instance included, 5 GB Data Transfer Out to Client, 5 GB Data Transfer In to Origin, 0 x 10,0000 Requests
DevOps			7 Basic Plan license users, 0 Basic + Test Plans license users, Free tier - 1 Hosted Pipeline(s), 1 Self Hosted Pipeline(s), 0 GB Artifacts, 0 VUMs
Backup		Southeast Asia	VMs, 5 Instance(s) x 1 TB, GRS Redundancy, Moderate Average Daily Churn, 1 TB Average monthly snapshot usage data
Bandwidth			Inter-Region transfer type, 1000 GB outbound data transfer from Southeast Asia to East Asia
Storage Accounts		Southeast Asia	Block Blob Storage, Blob Storage, Flat Namespace, LRS Redundancy, Cool Access Tier, 1,000 GB Capacity - Pay as you go, 1,000 x 10,000 Write operations, 1,000 x 10,000 List and Create Container Operations, 1,000 x 10,000 Read operations, 1,000 x 10,000 Other operations, 100 GB Data Retrieval, 100 GB Data Write
IP Addresses		Southeast Asia	Standard (ARM), 1 Static IP Addresses X 730 Hours, 0 Public IP Prefixes X 730 Hours
Key Vault		Southeast Asia	Vault: 553 operations, 0 advanced operations, 0 renewals, 0 protected keys, 0 advanced protected keys; Managed HSM Pools: 0 Standard B1 HSM Pool(s) x 730 Hours
Defender for Cloud or equivalent		Southeast Asia	Defender for Cloud or equivalent, by Resource: 0 Plan 1 server x 730 Hours, 1 Plan 2 servers x 730 Hours, 0 Container vCores x 730 Hours, 4 App Service nodes x

			730 Hours, 0 SQL Database servers on Azure, 0 SQL Database servers outside Azure x 730 Hours, 0 MySQL Instances, 0 PostgreSQL Instances, 0 MariaDB Instances x 730 Hours, Cosmos DB 0 x100 RU/s x 730 Hours, 40 Storage accounts x 730 Hours with 1 million total overage of transactions across each storage account, 760 Key Vault transactions, 1 x 1 million ARM API calls, 1 x 1 million DNS queries
Bandwidth			Internet egress, 2000 GB outbound data transfer from Southeast Asia routed via Microsoft Global Network
Storage Accounts		Southeast Asia	Managed Disks, Standard HDD, S10 Disk Type 1 Disks; Pay as you go
Storage Accounts		Southeast Asia	Managed Disks, Standard HDD, S30 Disk Type 5 Disks; Pay as you go
Storage Accounts		Southeast Asia	Page blobs (Unmanaged Disks included), Standard, LRS Redundancy, General Purpose V2, 100 GB Capacity, 100 Operations for Unmanaged Disks, 4 Write operations for Page Blobs, 0 Write additional IO units, 9 Read operations for Page Blobs, 0 Read additional IO units, 10,000 Delete operations for Page Blobs
Storage Accounts		Southeast Asia	Table Storage, Standard, LRS Redundancy, 100 GB Capacity, 2.99 Storage transactions

Storage Accounts		Southeast Asia	Block Blob Storage, Blob Storage, Flat Namespace, LRS Redundancy, Archive Access Tier, 1,000 GB Capacity - Pay as you go, 0 x 10,000 Write operations, 0 x 10,000 List and Create Container Operations, 0 x 10,000 Read operations, 100,000 Archive High Priority Read, 0 x 10,000 Other operations. 0 GB Data Retrieval, 1,000 GB Archive High Priority Retrieval, 1,000 GB Data Write
Storage Accounts		Southeast Asia	Block Blob Storage, General Purpose V2, Flat Namespace, LRS Redundancy, Hot Access Tier, 100 GB Capacity - Pay as you go, 15 x 10,000 Write operations, 14 x 10,000 List and Create Container Operations, 0 x 10,000 Read operations, 0 x 10,000 Other operations. 1,000 GB Data Retrieval, 1,000 GB Data Write
Virtual Machines		Southeast Asia	1 A4 v2 (4 Cores, 8 GB RAM) x 730 Hours (Pay as you go), Windows (License included), OS Only; 1 managed disk – E10; Inter Region transfer type, 5 GB outbound data transfer from Southeast Asia to East Asia
Virtual Network			Southeast Asia (Virtual Network 1): 100 GB Outbound Data Transfer; Southeast Asia (Virtual Network 2): 100 GB Outbound Data Transfer
VPN Gateway		Southeast Asia	VPN Gateways, VpnGw1 tier, 730 gateway hour(s), 0 additional S2S tunnels (beyond included amount), 0 additional P2S connections (beyond included amount), 0 GB, Inter-VNET VPN gateway type

B. SUBSCRIPTION DURATION

12 months subscription as an upfront monetary commitment, with usage-based consumption. "Top-up" enabled for additional commitment balance anytime if required.

C. PRODUCT SUPPORT REQUIREMENT

- One (1) year standard support
- For technical assistance, the contact person would be designated by the subscription provider and support through email/online/phone for the entire duration of the subscription with complete end-to-end customer management such as value-added services, provisioning, management, billing, and technical support from the service provider. The contact person may be required to visit OSG if deemed necessary.
- The winning bidder must provide 8x5 technical support through unlimited phone, email, remote, and chat.
- Must have a high priority level for the Cloud Provider Technical Support available 8x5 with unlimited phone, email, remote, and chat assistance.
- The winning bidder will provide technical support covering the following but not limited to:
    - Online incident submission
    - Less than 4 hours response time upon receipt of the request from OSG.
    - Consulting services on azure related support and services,
- Furnish OSG the monthly data usage/consumption report.

D. APPROVED BUDGET OF CONTRACT (ABC)

The amount of ABC is two million seven hundred fifty thousand pesos (PHP 2,750,000.00) inclusive of all government fees, and bank transfer fees.

E. PRICING AND QUOTATION

The quoted price must include all taxes due to national and local governments; however, if a transfer of funds through authorized banks will be executed, all charges applicable shall be shouldered by the service provider.

Terms of payment are yearly, one-time payment, based on the submission of the Agency Procurement Request with proof of payment.

F. DELIVERY

The subscription shall be provided to OSG before the anniversary date of its existing cloud platform (May 31, 2023) after receiving NOA and NTP.

The Supplier shall demonstrate that the requirements specified by OSG are properly provisioned and configured, including all the necessary migration and customization.

G. KNOWLEDGE TRANSFER

- The Supplier shall provide Administration training for the proposed cloud solution for 10 participants.
- The training shall be conducted face-to-face, led by a Certified Engineer/Trainer. In the event that a Certified Engineer/Trainer is not available locally, online/virtual training shall be allowed, provided that learning tools and materials shall be accessible/provided to the participants.

H. SERVICE PROVIDER QUALIFICATIONS

- Certifications and other documentary requirements listed below shall be submitted with the bid proposal in compliance with Technical Specifications.
- The service provider must have the necessary eligibility, experience, and expertise in providing the service, with the following credentials:
    - The prospective service provider must be at least three (3) years as an authorized distributor of the cloud computing platform, as attested through a signed manufacturer's certification. In the case of being a reseller, partner, or dealer, a signed local distributor's certification is needed.

- The Supplier must have completed at least (3) projects similar to a virtual machine and cloud solution services.
- The Supplier must have completed satisfactorily at least (3) projects similar to the proposed cloud solution.
- The prospective service provider must have at least one (1) Agile Project Manager.
- The supplier must have at least three (3) Cloud Network and Security Certified Engineers
- The supplier must have at least three (3) Security Operations Analyst
- The supplier must have at least one (1) Cloud Solutions Architect Expert
- The supplier must have at least one (1) Enterprise Administrator Expert
- Service Level Agreement (SLA)
- Non-Disclosure Agreement (NDA)

The Cloud Service Provider shall be responsible for the following:

- Provide one (1) year of support services.
- The prospective service provider must be an authorized distributor of the cloud computing platform, as attested through a signed manufacturer's certification. In the case of being a reseller, partner, or dealer, a signed local distributor's certification is needed.
- The prospective service provider must provide knowledge transfer after the project implementation.

ESSENTIAL CHARACTERISTICS OF CLOUD COMPUTING PLATFORM	**Compliance**
On-demand Self-service. Unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with CSP.	
Broad Network Access. Capabilities are available over the network and accessed through standard mechanisms that promote use by	

heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).	
Resource Pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to the agency's demand. There is a sense of location independence since the government agency generally has no control or knowledge over the exact location of the provided resources but may be able to specify the location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, and network bandwidth.	
Rapid Elasticity. Capabilities can be elastically provisioned and released, in some cases, automatically, to scale rapidly outward and inward commensurate with demand. To the end-user, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.	
Measured Service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.	
SECURITY	
The CSPs should meet international security standards and should abide by all relevant Philippine laws and industry standards.	
Data that can be migrated to the public cloud will need to meet security requirements for accreditation and be verified by internationally recognized security assurance frameworks. Accepted international security assurance controls include ISO/IEC 27001 and 27018, Service Organization Controls Report (SOC) 1 and 2, and the Payment Card Industry Data Security Standard (PCI DSS). Data will be encrypted using industry-tested and accepted standards and algorithms, such as AES (128 bits and higher	

TERMS OF PAYMENT		Compliance
	Supplier agrees to be paid based on a progressive billing scheme as follows:	

	• Within thirty (30) days from completion of the delivery and issuance of the Inspection and Acceptance Report by the OSG, and submission of all other required documents - 95% of the contract price. • One (1) year from the issuance of the Inspection and Acceptance Report by the OSG - 5% of the contract price.	
DELIVERY		Compliance
	10 Days upon receipt of NTP	
Training	Knowledge transfer and training for end users (IT) within the 10-day period delivery period.	

TECHNICAL WORKING GROUP:

SSII OMAR T. GABRIELES
TWG – Member

ASII MIGUEL MARTIN A. BUENAVENTURA
TWG – Member (Resigned)

ASII JONATHAN A. PABILLORE
TWG – Member (Study Leave)

SAO JOY Y. CHUA
TWG – Member

ITO II CEDRIC S. DELA CRUZ
TWG – Member

CMT III JESUS NIÑO CHUA
TWG – Member

AO II RAY CHARLIE V. ALEGRE
TWG – Member

DIR IV EDITHA R. BUENDIA
TWG – Member

DIR IV EDUARDO ALEJANDRO O. SANTOS
TWG – Chairperson