# PROCUREMENT OF PUBLIC CLOUD SERVICES FOR PHILSYS PROJECT

## 1. Procurement Objective

The Philippine Statistics Authority (PSA) 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.

## 2. Approved Budget for the Contract (ABC)

PSA, through the 2020 GAA Fund, intends to apply the sum of **ONE HUNDRED FORTY NINE MILLION & 00/100 Pesos (Php 149,000,000.00)** being the Approved Budget for the Contract (ABC) to payments under the contract for Procurement of Pubic Cloud Services for the Philippine Identification System (PhilSys) Project - System Integration Cloud Infrastructure Hosting Services. The ABC is the total budget allocated for the duration of the contract which is eight (8) monthswith option to renew, provided the Services rendered are of acceptable quality and cost-beneficial to PSA, 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.

## 3. Contract Duration

The initial engagement duration shall be for eight (8) months, upon full activation of the procured instances and shall likewise cover the connectivity service, Public IP and Technical Support Services.

## 4. Technical Specifications & Requirements

4.1. Cloud Infrastructure-as-a-Service (Iaas) Requirements

4.1.1. The Cloud Service provider must be ISO certified:

4.1.1.1. ISO 27001

http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

4.1.1.2. ISO 27017

http://www.iso.org/iso/catalogue_detail?csnumber=43757

4.1.1.3. ISO 27018

http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498

4.1.2. The CSP will need to meet security requirements and be verified by internationally recognized security assurance frameworks, such as but not limited to:

4.1.2.1. Service Organization Controls (SOC) Report 1

4.1.2.2. Service Organization Controls (SOC) Report 2

4.1.3. The account ownership and its related services shall belong to PSA. Access rights may be given to third party vendor(s), as deemed necessary, to perform any services related to the project. PSA however shall have the right and ability to revoke said rights at any given time from the root account.

4.1.4. The CSP shall provide, as part of the subscribed services, 24x7 Technical Support to all instances and resources subscribed by PSA. 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 1 hour from support ticket logging.

4.1.5. Shall Provide an interactive Graphical User Interface (GUI) with 2-Factor Authentication that allows user to manage all hosting service instantly and securely.

4.1.6. Must have the capability to deploy a Highly Available and Multi-Zone Disaster Recovery enabled solution across multiple datacenters within ASEAN Region. 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. Capability to deploy across multiple sites shall be made available through a self-service portal with a Graphical User Interface (GUI).

4.1.7. 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 and High Availability failover.

4.1.8. 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.

4.1.9. Must Provide a dashboard for cloud administrators which shall provide an overall view of the size and status of the subscribed Cloud Environment.

4.1.10. Must provide an Application Centric Infrastructure (ACI) multi-site orchestrator which will provide visibility onto a cloud environment.

4.1.11. Shall provide performance monitoring capabilities for processor, memory, disk usage, and network utilization.

4.1.11.1. The performance Monitoring component shall provide tools and means to actively capture performance-related information of Cloud Environment services or resources.

4.1.11.2. The performance Monitoring tool must have the ability to send customizable email notifications to administrations based on threshold alarms.

4.1.11.3. The performance Monitoring components must have the ability to capture initial performance baseline which can be used to analyze the variation in performance of the services.

4.1.11.4. 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.

4.1.12. Isolated Private Network and Private Cloud Options:

4.1.12.1. All cloud instances and services must be hosted within an isolated private network or virtual private cloud that can support up to 50Tb per month data transfer out from the cloud.

4.1.12.2. The Service Provider must have the ability/option to provide dedicated virtual machines and hosts should PSA decides the need for it.

4.1.12.3. Must be able to support IPv6 Protocol.

4.1.13. The CSP must be able to engage in an On-Demand or Pay-per-Use Model where PSA will pay based on actual usage and not based on reserved instances. The CSP shall provide capability to ensure access to additional resource capacity based on incremental requirements at any given time.

Additionally, the incremental requirements for cloud resources may go beyond the initially subscribed services but within the Service Catalog of the CSP.

4.1.14. Data Sovereignty

4.1.14.1. PSA 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.

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

4.1.14.3. The CSP 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 PSA.

4.1.15. Must provide built-in audit logging features that capture all API requests/changes to the infrastructure for audit purposes. PSA shall have the ability to determine the retention length for these audit logs.

4.1.16. Must provide a template-based service to simplify deployment and eliminate the need to deploy individual elements of an application. This service must allow the end-user administrator, and its contractors (if any), to input and save the infrastructure setup to allow effective and efficient redeployment in the event of an error.

4.1.17. To guarantee government regarding with the reliability of the Cloud Solution being offered, the Cloud Service Provider must be a leader in Gartner's IaaS Magic Quadrant for at least three (3) consecutive years.

4.1.18. PSA requires the Cloud Service 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 PSA's procurement of the said service.

4.2. Compute and Storage Sizing Requirements

4.2.1. As stated in Section 4.1.13. of this document, PSA shall engage the CSP 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 PSA on Day 1 and shall be adjusted depending on the resources demand of the project.

4.2.2. The initial sizing required is tabulated below:

| Server Type | Qty | vCPU | Memory (GiB) | Total vCPU | Total Memory | Duration (Months) |
|---|---|---|---|---|---|---|
| Instance_1 | 4 | 4 | 32 | 16 | 128 | 8 |
| Instance_2 | 2 | 2 | 16 | 4 | 32 | 8 |
| Instance_3 | 2 | 2 | 16 | 4 | 32 | 8 |
| Instance_4 | 2 | 2 | 16 | 4 | 32 | 8 |
| Instance_5 | 8 | 8 | 32 | 64 | 256 | 8 |
| Instance_6 | 16 | 16 | 32 | 256 | 512 | 8 |
| Instance_7 | 8 | 8 | 32 | 64 | 256 | 8 |
| Instance_8 | 8 | 8 | 16 | 64 | 128 | 8 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Instance_9 | 8 | 8 | 32 | 64 | 256 | 8 |
| Instance_10 | 16 | 16 | 32 | 256 | 512 | 8 |
| Instance_11 | 8 | 8 | 32 | 64 | 256 | 8 |
| Instance_12 | 4 | 4 | 32 | 16 | 128 | 8 |
| Instance_13 | 15 | 8 | 64 | 120 | 960 | 8 |
| Instance_14 | 1 | 96 | 384 | 96 | 384 | 8 |
| Instance_15 | 1 | 96 | 384 | 96 | 384 | 8 |

| **Raw Block-Level Storage (Gen-Purpose SSD) – (Tb)** | **Object Storage (Tb)** | **Data Transfer Out per Month (TB)** | **IOPS** |
|---|---|---|---|
| 228 | 200 | 40 | 100/GB |

4.3. Must provide a Cloud-based Hardware Security Module (HSM).

4.3.1. Must be single-tenant and tamper resistant

4.3.2. Must support FIPS 140-2 Level 3 standard for cryptographic modules.

4.3.3. Must be configured in a cluster (4 clusters, 2 nodes per cluster) providing high availability and load balancing features, with key replicated across HSMs within the cluster

4.3.4. Must be able to support on-demand scaling using the CSPs graphical user interface (GUI) or Command-line Interface (CLI)

4.3.5. Must offer integration with custom applications via industry-standard APIs and supports multiple programming languages, including PKCS#11, Java Cryptography Extensions (JCE), and Microsoft CryptoNG (CNG) libraries

4.3.6. Must support quorum authentication for critical administrative and key management functions

4.3.7. Must support multi-factor authentication (MFA)

4.3.8. Must be a CSP managed service, eliminating tasks such as hardware provisioning, software patching, high availability configuration, and backups. Must support 2048, 4096 bit RSA Private Keys, 256 bit AES keys on FIPS 140-2 Level 3 Certified Memory of Cryptographic Module.

4.4. Infrastructure Security Requirements

4.4.1. Encrypted Audit Trail/Logs

4.4.1.1. Must support multi-factor authentication deletes for unintentional deletes and additional security

4.4.1.2. Able to support audit trail and deliver logfiles to the CSP's object store for secure access

4.4.1.3. Able to support audit trail for both graphical user access (GUI) events and command-line interface (CLI) events

4.4.1.4. Must support granular access control through user policies and/or object storage bucket policies

4.4.2. Web Application Firewall (WAF)

4.4.2.1. 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.

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

4.4.3. Cloud Distributed Denial of Service (DDoS) Protection

4.4.3.1. 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.

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

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

4.4.4. Security Compliance Assessment

4.4.4.1. Able to provide threat detection service that constantly monitors malicious activities and unusual/unauthorized behavior to protect cloud accounts, workloads, and data stored in the cloud object store.

4.4.4.2. Must provide analysis on continuous streams of meta-data generated from accounts and network activities found in audit trails, network flow logs, and DNS logs.

4.4.4.3. Able to provide built-in detection techniques for reconnaissance, instance compromise, account compromise and object storecompromise.

4.4.5. Secured Monitoring

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

4.4.5.2. Must support access through APIs, Command Line Interface (CLI), programming software development kits (SDKs), and the CSP's management console.

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

4.4.5.4. Must be able to create metric dashboards.

4.4.5.5. Able to support isolation and analysis of performance issues impacting container environment i.e. Kubernetes clusters.

4.4.6. Configuration Rules

4.4.6.1. Able to provide capability to assess, audit, evaluate configurations of cloud resources.

4.4.6.2. Able to capture and record configuration changes in any of the cloud resources.

4.4.6.3. Must provide pre-built rules for evaluating, provisioning, and configuring of cloud resources.

4.4.6.4. Must support customization of pre-built rules.

4.4.6.5. Must support conformance packs by putting together common frameworks that can be deployed across entire organizations.

4.4.6.6. Able to provide compliance dashboards from defined rules/packs.

4.5. Cloud Connectivity Requirements

4.5.1. Dedicated Connectivity

4.5.1.1. Must provide redundant, dedicated, private cloud connectivity to the off-shore Cloud Infrastructure.

4.5.1.2. Must eliminate Single Points of Failures (SPOF) covering submarine cables, landing points, telecommunication providers and physical network devices.

4.5.1.3. Must provide a minimum bandwidth of 1GB to the off-shore Cloud Infrastructure from the on-premise data centers.

4.5.1.4. Supports Border Gateway Protocol (BGP) for up to 100 advertised routes.

4.5.1.5. Supports 1000BASE-LX or 10GBASE-LR connections over single mode fiber using ethernet transport.

4.5.1.6. Support for devices with 802.1Q VLANs.

4.5.1.7. Must follow the CSP maximum resiliency recommendations.

4.5.1.8. Supports Bi-directional Forwarding Detection (BFD) for fast failure detection and failover.

4.5.1.9. Must have an availability SLA of 99.9%.

4.5.2. Virtual Private Network (VPN)

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

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

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

4.5.3. Internet Connectivity

4.5.3.1. The winning bidder shall provide a minimum of 1Gbps internet connectivity for each of the PSA identified data centers, including all essential peripherals.

4.5.3.2. Must have a minimum availability SLA of 99.9%.

4.6. Centralized Application Logs Requirements

4.6.1. Search and Log Analytics Engine

4.6.1.1. Fully managed open-source, RESTful, distributed search engine to store, search, and analyze application logs.

4.6.1.2. Should offer REST based APIs, HTTP interface, and schema-free JSON documents.

4.6.1.3. Supports Java, Python, PHP, JavaScript, Node.js, Ruby programming languages.

4.6.1.4. Provides integrated open-source visualization and reporting tool, Kibana (https://github.com/elastic/kibana).

4.6.1.5. Managed through the cloud service providers graphical user interface (GUI) or command line interface (CLI).

4.6.1.6. Supports built-in event monitoring and alerting.

4.6.1.7. Supports querying using SQL syntax.

4.6.1.8. Supports deployment across multiple cloud data centers or availability zones for availability and fault tolerance.

4.6.1.9. Durability via automated and manual snapshots.

4.6.1.10. Snapshots are stored in the cloud providers object storage designed for 11 9's of durability.

4.6.1.11. Supports cloud providers IP-based security policies, access control through user policies, or basic authentication with username and password.

4.6.1.12. Supports encryption for data-at-rest and data-in-transit.

4.6.1.13. Search engine must support magnetic, general purpose solid state drives (SSD) by specifying storage capacity, or IO optimized solid state drives (SSD) by specifying disk IOPs.

4.6.1.14. Supports no-downtime scaling (adding or modifying instances).

4.6.1.15. Logs performance metrics of the search engine to the cloud service providers centralized performance metric logs.

4.6.1.16. The log engine shall have 16 vCPUs with and 128 GiB of memory per node

4.6.1.17. The log engine shall have a minimum of two nodes in a cluster for high availability

4.6.2. Log Processor

4.6.2.1. Supports data ingestion through the cloud providers data ingestion service, or open-source data ingestion tools such as:

4.6.2.1.1. Logstash (https://github.com/elastic/logstash)

4.6.2.1.2. Fluentd (https://github.com/fluent/fluentd)

4.6.2.1.3. Fluentbit (https://github.com/fluent/fluent-bit)

4.6.2.2. Log processor should be able to process containers logs from the file system or Systemd/Journald.

4.7. Data Sovereignty, Data Residency and Data Privacy Compliances

4.7.1. The CSP is required to comply with Data Sovereignty Guidelines and Policies as prescribed in the Philippine Government's Cloud First Policy:

4.7.1.1. 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.

4.7.1.2. 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 CSP, 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 CSP.

4.7.1.3. CSP 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.

4.7.2. The CSP 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:

4.7.2.1. The Philippine Territory.

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

4.7.2.3. 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:

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

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

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

4.8. 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, PSA 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% |

4.9. The CSP shall provide an enterprise support plan that will deliver the following:

4.9.1. 24x7 phone, email, and chat access to Cloud Support Engineers

4.9.2. Designated Technical Account Manager (TAM) to proactively monitor the subscribed environment and assist with optimization

4.9.3. Well-Architected Reviews

4.9.4. Concierge Support Team

## 5. Cloud Administration Services

5.1. Implementation services for all cloud components proposed by the provider

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

5.3. The provider will monitor system and resource alerts, resource utilization and resource contention to support the environment

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

5.5. As part of the service improvement plan, the provider will provide PSA recommendations on cost optimization.

5.6. Provider will report on start and stop times for data transfer jobs to the cloud on a monthly basis.

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

5.8. The bidder providing the cloud administration services must be ISO 9001:2015 certified

5.9. The bidder providing the cloud administration services must be ISO/IEC 27001:2013 certified

## 6. Cloud Infrastructure Training

6.1. The winning bidder provide end-user training from CSP accredited trainers/instructors.

6.2. The winning provider will provide training on the following topics for X number of PSA nominated participants:

6.2.1. Architecting for the chosen CSP

6.2.2. Advanced Architecting for the chosen CSP

6.2.3. System Operations for the chosen CSP

6.2.4. Security Engineering for the chosen CSP

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

## 7. Payment Milestones/Terms

PSA shall pay it subscription on a monthly basis based on actual usage, as defined in Section 4.1.13 of this document. Other payment conditions are as follows:

7.1. The accumulated payables within the validity of the Subscription Period must not exceed the ABC set for this procurement.

7.2. All activated additional resources must be billed not less than 30 calendar days from date of activation or 60 calendar days should it be activated beyond the agreed "cut-off" period.

7.3. All chargeable costs must be inclusive of VAT.