Republic of the Philippines
DEPARTMENT OF SCIENCE AND TECHNOLOGY
Philippine Atmospheric, Geophysical and Astronomical Services Administration (PAGASA)

TERMS OF REFERENCE FOR SUPPLY, DELIVERY, TESTING AND INSTALLATION OF PAGASA API CLOUD INFRASTRUCTURE SERVICE AND FIREWALL

A. BACKGROUND

The Engineering and Technical Services Division - Meteorological Equipment, Telecommunications and Technical Services Section (ETSD-METTSS) at PAGASA, which oversees the maintenance and development of the PAGASA Application Programming Interface (API), is set to acquire a cloud infrastructure service. This API serves as the pivotal data source for both the PAGASA Website and the PANAHON Website. It is also extensively utilized by various other government and non-government agencies, who depend on it as the authoritative source for weather and climate data. This strategic move to a cloud infrastructure is aimed at bolstering the reliability, accessibility, and scalability of these critical data services.

The existing on premise infrastructure for the PAGASA API is currently supported by a single, large physical server. While this server is adequately sized to manage our present workload, it lacks a robust, efficient, and cost-effective method for scaling. Considering our commitment, along with that of other agencies, to achieve 99.9% availability, it is imperative for PAGASA to transition from this limited on premise setup to a more scalable and reliable cloud-based infrastructure. This migration will significantly enhance our capacity for handling increasing workloads and ensuring consistent availability, aligning with our operational objectives and service commitments.

The PAGASA API Cloud Infrastructure is being designed as a comprehensive and robust system, encompassing several key components to ensure optimal performance and reliability. This infrastructure will include a dedicated web server for handling client requests, a database server optimized for fast and secure data retrieval and storage, and a cache server to enhance data access speed and efficiency. Additionally, a file server will be incorporated for organized storage and management of digital files. To ensure seamless distribution of network traffic and prevent overload, a load balancer will be a crucial part of the setup. Finally, integrating a Content Delivery Network (CDN) will significantly improve content delivery speed by caching data in multiple, geographically diverse locations, thereby ensuring faster access for users regardless of their location. Together, these elements will form a robust and scalable cloud infrastructure, tailored to meet the high demands and reliability standards of PAGASA's data services.

B. APPROVED BUDGET FOR THE CONTRACT (ABC)

The Approved Budget for the Contract is **Three Million Two Hundred Thousand Pesos (3,200,000.00)** inclusive of VAT and all applicable government taxes.

C. DELIVERY PERIOD AND PLACE OF DELIVERY

The winning bidder shall provide Cloud Infrastructure to ETSD-METTSS within 30 calendar days from receipt of the Notice to Proceed at PAGASA Central Office located at PAGASA Science Garden Complex, Senator Miriam Defensor Santiago Ave., Brgy. Central, Quezon City.

D. TECHNICAL SPECIFICATIONS AND REQUIREMENTS

The winning bidder shall provide **Twelve (12) Months** of cloud infrastructure services and **One (1) Integrated Firewall Solution.**

The **Integrated Firewall Solutions** should have the following minimum specifications.

- Physical Interface
  - At least 6x 10/100/1000 BASE-T Interfaces
  - At least 4x10GE Fiber SFP+ Interfaces
  - At least 2x USB Ports
  - At least 1x Serial Port
- Performance
  - Firewall Throughput – 2.8 Gbps
  - NGFW Throughput – 2.5 Gbps
  - WAF Throughput – 2.5 Gbps
  - IPS & WAF Throughput -1.4 Gbps
  - Threat Protection Throughput -1.8Gbps
  - IPsec VPN Throughput - 250Mbps
  - Max IPsec VPN Tunnels – 300
  - Concurrent TCP Connections – 750,000
  - New TCP Connections – 20,000
- Hardware
  - RAM - 4GB
  - Storage HD Capacity – 64G SSD
  - Power - 40W
  - Operating Temperature - 0-45*C
- Must support policy configuration modules for the following functions from a single appliance:
  - IPSec Virtual Private Network (IPVPN)
  - Secure Sockets Layer Virtual Private Network (SSLVPN)
  - Proprietary Virtual Private Network (VPN)
  - Software-Defined Wide Area Network (SDWAN) Capability
  - Web Application Firewall (WAF)
  - Anti-Virus/Malware (AV)
  - Intrusion Prevention System (IPS)
  - Real-time Vulnerability Scanner
- Must provide an on premise URL signature database for URL Filtering, not only rely on cloud
- Must support anti-virus feature that scan the files up to 20MB.
- Must support anti-virus feature with compressed file detection, and support compress file with up to 16 layers.
- Must provide risk analytics module that allows to scan and identify security loopholes such as open port, system vulnerabilities, weak passwords, etc
- Must have risk assessment that support major protocols such as HTTP, HTTPS, POP3, SMTP, RDP, SMB, Oracle, MSSQL, MySQL etc.
- Must include the local hard disk to provide log retention and report creation of at least 30 days
- Must have SD-WAN capability via VPN tunnels:

    - Can provide intelligent or dynamic path selection
    - Can choose the optimize link based on bandwidth-remaining ratio, application type or link quality (means packet loss, jitter, latency).
- Must able to support multiple ISPs for SD-WAN.
- Must support WAF feature by itself, without additional devices. The WAF protection should meet at least the following specifications:
    - Must be able to support the attack types, such as XSS, SQL, CSRF, CC attack, OS Command Injection, Web shell, scanner blocker, path transversal etc.
    - Be able to defense OWASP top 10 attacks
    - Support WAF related signature on premise no less than 4500 signatures and support customize signature.
    - Support HTTPS site protection with decryption enabled.
    - Support weak password detection for web-based applications.
    - Support CC attack protection
    - Support HTTP request Anomaly detection, SQL injection in HTTP header, POST entity overflow, HTTP header overflow, etc.
- Must provide a real-time vulnerability analysis or passive vulnerability scan:
    - Detection vulnerabilities based on traffic pass through, without any active scanning activities to the servers, minimize the extra work load and other impact
    - The vulnerabilities that can be detected includes web application vulnerability, weak password, improper configuration on web server, etc.
    - Support generate HTML format report
- Must support ACL policy optimizer, which helps:
    - Identify the redundant policy, expired policy, conflict policy etc.
    - Be able to track the ACL policy life cycle, help to track every change that have been done to the ACL policies.
- Must support a dedicated ransomware protection module, which can:
    - Automatically scan and detect ransomware related vulnerabilities, port, weak password, brute-force attack etc.
    - Provide dedicated GUI page to show and respond all the ransomware related vulnerabilities
    - Can provide guidance or suggested action to admin, e.g., deploy block policy direct
- Must support a dedicated dashboard to summarize business system(server) relate security risks, the information provide via dashboard includes:
    - Business system severity level, attack events, vulnerabilities.
    - Stages of Attack to let IT admin understand the security impact
    - One-click to block attackers IP
- Must support a dedicated dashboard to summarize user relate security risks, the information provide via dashboard includes:
    - User severity level, attack types, attack events
    - Stages of Attack to let IT admin understand the security impact
- Must support building a proprietary virtual private network (VPN) tunnel with the existing Head Office Firewall to ensure the security, interoperability, and ease of management
- Must support implementing security policies coming from a central manager that can manage remote offices and the existing head office firewall thus ensuring compatibility and interoperability.
- To ensure the maturity of solution technology, the principal must be CMMI L5 certified

- The proposed solution must be in level of Magic Quadrant for Network Firewalls 2022.
- To ensure the maturity of solution technology, the supplier/manufacturer must have the following certification:
    - ISO 9001:2015
    - ISO/IEC 27001:2013
    - ISO 14001:2015
    - ISO/IEC 20000-1:2018
- Partner/reseller for the proposed solution should have technical certification from the principal/vendor.
- Peripherals
    - 2 x 10GB SFP+ Transceiver
- License for 1 year

The **Cloud Infrastructure Service** to be provided should have the following minimum specifications:

- Compute Resources:
    - API Servers: Minimum 2 instances, scalable up to 4;
    - Specifications: 8vCPU, 32GB RAM
- Bastion Server
    - Minimum 1 instance
    - Specifications: 1vCPU, 2GB RAM
- Database Server:
    - Specifications: 4vCPU, 15GB RAM
- Cache Server:
    - Specifications: 2vCPU, 6.42 GB RAM
- Storage:
    - API Servers: 200 GB each
    - Bastion Server: 20 GB each
    - Database Server: 500 GB
    - S3 Storage: 1 TB per month
- Networking:
    - Load Balancer: Application Load Balancer
        - Capacity: 100 GB monthly traffic
        - Throughput: 100 connections per second
    - Content Delivery Network:
        - Transfer Out: 1 TB/month to Internet, 1 TB/month to Origin
    - Domain Management
        - 4 Hosted Zone
    - Virtual Private Cloud (VPC) for secure network setup

Two (2) Mid-range Laptop

- Display - 15 to 16.9 inches
- Processor - 6 cores or better
- Graphics - 6GB Dedicated VRAM or better
- Memory - 24GB RAM or better
- Storage - 512GB SSD or better

PERFORMANCE AND SCALABILITY

- Auto Scaling: Based on user demand, with a minimum of 2 and maximum of 4 instances.
- Load Balancing: To distribute traffic evenly across servers and maximize

uptime.

- High Availability: Target 99.95% uptime for cloud services.

SECURITY REQUIREMENTS

- Web Application Firewall: 1 Web ACL, 10 rules/month
- Security Access Policies: For object store and data protection.
- Encryption: In transit and at rest.
- Compliance: Adherence to relevant data protection and privacy regulations.

MIGRATION AND INTEGRATION REQUIREMENTS

- Seamless migration/replication of existing on-premises/cloud to the infrastructure service.
- Database migration and replication with minimal downtime.

MONITORING AND MANAGEMENT

- Cloud monitoring for logs, insights, events, and alarms.
- Web-based console for resource management.

SUPPORT AND MAINTENANCE

- 24/7 cloud engineer support.
- Guaranteed response time of less than 1 hour.
- Guaranteed response time of less than 30 minutes during inclement weather.

DOCUMENTATION

- Comprehensive documentation of the infrastructure setup, configuration.

COMPLIANCE AND STANDARS

- All components and services must comply with industry standards and best practices.
- Auto scale service based on user demand.

E. SCOPE OF WORK

Infrastructure:

- Configure compute resources, storage, and network components.
- Configure security measures, including firewalls, encryption, and access controls.

Database Migration:

- Real-time database replication to cloud-based managed relational database system.

Performance Optimization:

- Ensure auto-scaling capabilities for handling varying loads.

- Optimize database and server performance for high availability and redundancy.

Monitoring and Management:

- Real-time cloud monitoring.
- Routing system checks and maintenance.

TURN OVER

- Cloud User Account Transfer

F. SERVICE LEVEL AGREEMENT

Cloud Service

- The Cloud Service Provider shall ensure that the cloud platform is available with a monthly uptime percentage of at least 99.95% during any monthly billing cycle as a "Service Commitment".
- Technical Support must be available 24 x 7 days.
- Technical Support must be on standby during inclement weather.

Hardware

- 24/7 technical support should be available via phone and onsite during the contract period.
- Defective ICT equipment should be repaired within 48 hours, with parts replaced free of charge if found defective in materials or workmanship under normal and proper use.
- The winning bidder must provide a service unit during any equipment failures.
- If the ICT hardware cannot be repaired due to difficulties and requires removal, the winning bidder must provide a replacement unit.

The bidder warrants that it shall strictly conform to all the Terms and Conditions of this Terms of Reference.

G. HARDWARE WARRANTY

- All equipment shall be warranted by the winning bidder for three years. The winning bidder shall provide replacement of new units within 30 calendar days from the date of notification for all defective and factory defect equipment at no cost to PAGASA. The winning bidder shall arrange and pay for the return of the defective unit(s) and the shipping of new replacement unit(s) to PAGASA.

H. SITE ACCEPTANCE

- Two (2) supervisory personnel from PAGASA ICT and Inspection Committee shall conduct and assist in the acceptance procedure and signing of site acceptance certificate. The acceptance procedure and signing shall be conducted after the testing and commissioning. Meals shall be provided by the winning bidder during the conduct of acceptance (breakfast, morning coffee break, lunch and afternoon coffee break).

I. GENERAL NOTE

- The winning bidder must provide a warranty certificate covering the ICT equipment delivery
- The winning bidder must have a certified true copy of a valid certificate of distributorship/dealership/reseller ship or professional partnership with the distributor/manufacturer of the brand for Integrated Firewall Solution.
- The winning bidder must assign minimum of two personnel to assist the PAGASA ICT in unboxing, installation of software until the duration of inspection.
- Quality assurance is expected from the winning bidders, such that any error or fault in any hardware, peripherals, preinstalled mandatory software and installation tools delivered during the implementation shall acted upon, resolved, mitigated and/or replaced accordingly at no cost to the PAGASA. Likewise, upon final project acceptance, the winning bidder is required to provide aftersales service and assurance that all equipment and installation are accurate, complete, operable, uncompromised and error-free during warranty.
- All components are branded and should be factory installed with corresponding part number.