



COOPERATIVE DEVELOPMENT AUTHORITY

827 Aurora Blvd., Service Road, Brgy. Immaculate Concepcion, Cubao, 1111 Quezon City, Philippines

cda.gov.ph

helpdesk@cda.gov.ph

CDA Philippines



International Year of Cooperatives

Cooperatives Build a Better World

REQUEST FOR QUOTATION

Date: December 5, 2025
RFQ NO. 2025 - 309

Name of Company: _____
Address: _____

Business Permit No.: _____
TIN: _____

Please quote your best offer for the item/s described below, subject to the Terms and Conditions provided at the dorsal portion of this request for quotation. Submit your quotation duly signed by you or your duly authorized representative not later than _____.


JOSELITO O. HALLAZGO
Chairman, Bids & Awards Committee

After having carefully read and accepted the Terms and Conditions, I/we submit our quotation/s for the item/s as follows:

ITEM DESCRIPTION	Quantity (QTY)	Approved Budget for the Contract	OFFER					REMARKS
			PRICE			Compliance with Technical Specifications (please check)		
			QTY	Unit Price	Total Price	Yes	No	
PURPOSE: FOR THE OFFICIAL USE OF CDA HEAD OFFICE - ICTD		₱377,755.39						
SUBSCRIPTION RENEWAL OF BUSINESS-GRADE CONTENT DELIVERY NETWORK (CDN) AND DISTRIBUTED DENIAL OF SERVICE (DDOS) MITIGATION TOOL FOR THE COOPERATIVE DEVELOPMENT AUTHORITY (CDA) 1. PROJECT DESCRIPTION 1.1. The Cooperative Development Authority (CDA) seeks a one-year subscription renewal of a business-grade Content Delivery Network (CDN) service with integrated DDoS mitigation, certificate management, and training. The subscription is intended to improve the speed, reliability, and security of CDA's digital services, ensuring seamless online operations, enhanced data security, and better stakeholder access nationwide. 2. SCOPE OF WORK AND SERVICES 2.1. The Provider shall provide the following services: 2.1.1. Business-Grade Subscription 2.1.1.1. A one (1) year subscription to a business-grade CDN service with integrated DDoS mitigation and certificate management capabilities. 2.1.2. Initial Setup and Integration 2.1.2.1. Configuration of CDA's domain and DNS settings within the CDN platform. 2.1.2.2. Setup of account structures, access permissions, and user controls. 2.1.3. Security Configurations 2.1.3.1. Activation of DDoS protection against application-layer and volumetric attacks. 2.1.3.2. Configuration of a Web Application Firewall (WAF) with a set number of customizable rules. 2.1.3.3. Implementation of SSL/TLS encryption for secure data exchange. 2.1.4. Performance Optimization 2.1.4.1. Activation of content caching to optimize website load times globally. 2.1.4.2. Configuration of caching policies and page rules for enhanced performance. 2.1.5. Traffic Management and Access Control 2.1.5.1. Implementation of rate-limiting to manage traffic loads and protect against bot attacks. 2.1.5.2. Configuration of IP filtering and geographic access controls as needed. 2.1.6. Monitoring and Alerts 2.1.6.1. Enable monitoring tools, including dashboards, logs, and real-time alerts. 2.1.6.2. Configure notifications for potential performance or security incidents. 2.1.7. Testing and Validation	1 LOT							

2.1.7.1. Conduct functional tests for security, performance, and configuration efficacy.

2.1.8. Documentation and Training

2.1.8.1. Provide comprehensive documentation on system configurations and procedures.

2.1.8.2. Deliver training to up to CDA personnel on system use and incident management.

3. TECHNICAL REQUIREMENTS

3.1. Performance

The solution must include:

3.1.1. Global Content Delivery Network (CDN) caching for accelerated content delivery.

3.1.2. Static content caching with instant full-cache purging and minimum cache TTL expiry of one second.

3.1.3. Support for modern protocols and technologies, including IPv6, HTTP/2, SPDY, and WebSockets.

3.1.4. Tiered caching to optimize resource delivery and reduce origin server load.

3.1.5. Network optimization tools for faster response times and reduced latency.

3.2. Customization & Optimization

The solution must offer:

3.2.1. Up to 50 configurable page rules for customizing traffic handling and caching behavior.

3.2.2. Accelerated mobile page (AMP) support to improve mobile web performance.

3.2.3. Asynchronous JavaScript loading to improve page performance.

3.2.4. Tools for managing and optimizing mobile-specific content.

3.2.5. CNAME setup for custom domain support.

3.3. Security

The solution must include:

3.3.1. Comprehensive DDoS protection for application-layer and volumetric attacks, including unmetered mitigation capabilities.

3.3.2. Advanced threat detection using reputation-based intelligence to identify and block emerging threats.

3.3.3. Protection against bot attacks (Basic bot management tools, like CAPTCHA and JavaScript challenges, are included.)

3.3.4. Mitigation against content scraping and spam through intelligent filtering mechanisms.

3.3.5. Real-time alerts for potential DDoS and other security incidents.

3.4. Certificate Management

The solution must provide:

3.4.1. Centralized management of SSL/TLS certificates with automated issuance and renewal.

3.4.2. Support for both universal SSL certificates and user-provided certificates.

3.5. Web Application Firewall (WAF)

The solution must include:

3.5.1. Web Application Firewall (WAF) with up to 100 customizable rules.

3.5.2. Free managed rulesets, including OWASP Core Ruleset, to protect against common vulnerabilities.

3.5.3. Security analytics for visibility into threats and potential vulnerabilities.

3.6. Reliability

The solution must include:

3.6.1. Global Anycast DNS with DNSSEC support for secure and efficient domain resolution.

3.6.2. Custom nameservers and wildcard DNS record proxying.

3.6.3. One (1) waiting room feature to manage traffic surges during high-demand periods.

3.7. Load Balancing (New Section)

The solution must include advanced load balancing features to ensure high availability and optimal performance across CDA web applications and services.

3.7.1. Global load balancing to distribute traffic across multiple origins or data centers for redundancy and reliability.

3.7.2. Application load balancing with health checks to automatically reroute traffic away from unresponsive or degraded origins.

3.7.3. Session affinity ("sticky sessions") support for maintaining user connections during active sessions.

3.7.4. Weighted load distribution for intelligent traffic allocation based on origin performance.

3.7.5. Failover and disaster recovery configurations to maintain service continuity during outages.

3.7.6. Support for DNS-based and Layer 7 (HTTP/HTTPS) load balancing.

3.7.7. Integration with CDN caching and DDoS protection layers for end-to-end performance and resilience.

3.8. Dashboard, User, and API Access

The solution must provide:

3.8.1. Multi-user administrative access with role-based access controls and read-only options.

3.8.2. API access and Terraform integration for automation and customization.

3.9. Insights & Analytics

The solution must provide:

3.9.1. Real-time analytics for traffic, caching, and security events.

3.9.2. Historical analytics with configurable resolutions (e.g., 15 minutes for site analytics, 7 days for DNS analytics).

3.9.3. Exportable logs and audit data in CSV format for further analysis.

3.9.4. Integrated dashboards for monitoring website performance.

3.10. Compliance

The solution must adhere to the following standards:

3.10.1. ISO 27001 certification.

3.10.2. SOC 2 Type II compliance.

3.10.3. PCI DSS 4.0 compliance for payment data security.

3.11. Support

The solution must include:

3.11.1. 24/7 support via ticketing and live chat.

3.11.2. Service Level Agreement (SLA) for uptime, with corresponding service credits for breaches.

3.12. Additional Scope

The Provider must also provide:

3.12.1. Advanced certificate management tools for enhanced SSL/TLS operations.

3.12.2. Training sessions for ICTD personnel on system operations, performance optimization, and incident management.

4. BUDGET AND RESOURCES

4.1. Approved Budget for the Contract (ABC):

4.1.1. The approved budget for the one-year subscription is Three Hundred Seventy Seven Thousand, Seven Hundred Fifty Five Pesos and Thirty Nine Centavos (PHP377,755.39) inclusive of all applicable taxes, fees, and other charges. Chargeable against the 2026 ICTD Funds.

5. PRE-TERMINATION

5.1. In case of pre-termination, the Provider shall be liable to additional liquidated damage equivalent to one percent (1%) of the contract price as provided by the Government Accounting Manual (GAM) and forfeiture of the Performance Security; and

5.2. The CDA shall have the right to blacklist the Provider in case of pre-termination.

6. WARRANTIES OF THE PROVIDER

6.1. The Provider warrants that it shall conform strictly to the terms and conditions of this TOR;

6.2. The Provider in the performance of its services shall secure, and maintain at its own expense all registration, licenses, or permits required by National or Local Laws and shall comply with the rules, regulations, and directives of Regulatory Authorities and Commissions; and

6.3. The Provider shall neither assign, transfer, pledge, nor sub-contract any part or interest therein.

7. MODE OF PAYMENT:

7.1. 100% payment upon the successful completion of the configuration, confirmation of the solution's readiness for use by CDA, and submission of proof of renewal or order fulfillment.

8. DELIVERY PERIOD

8.1. For the renewal of the subscription, the delivery and configuration of solutions, ensuring readiness for CDA's use, shall align with the subscription and warranty period from January 18, 2026, to January 18, 2027.

9. SUBSCRIPTION AND WARRANTY PERIOD

9.1. January 18, 2026 to January 18, 2027

10. ELIGIBILITY OF THE BIDDERS

10.1. PhilGeps registered;

10.2. The provider should be in the IT business for 5 years;

10.3. Capability for 24 x 7 customer/technical support;

10.4. The Provider MUST be a Value-Added Service (VAS) registered provider under the National Telecommunication Commission (NTC);

10.5. The Provider MUST be a current and authorized reseller or distributor of the solution;

10.4. The Provider MUST be a DICT-recognized or accredited cybersecurity provider.

11. OTHER TERMS AND CONDITIONS

11.1. The services required are classified as highly technical and the Provider shall perform or deliver these services with utmost professionalism. The Provider is prohibited from disclosing or disseminating any information, data owned by The CDA or gathered in any manner in the performance or delivery of services. This prohibition shall be effective even after the termination of the contract;

11.2. An independent Provider with no employer-employee relationship exists between the Provider and CDA. Any and all claims for compensation, death, unpaid wages, overtime pay, separation pay, damages of the Provider, heirs, beneficiaries, and/or assigns, as well as compliance with applicable laws and ordinance relating to the services to be performed under the contract, shall be the exclusive, direct and sole responsibility of the Provider;

11.3. The Provider shall hold CDA free and harmless from any liability, injury, disability, or death sustained by him or by third parties arising out of or in connection with the performance of the undertaking under the contract;

11.4. Neither the CDA nor the Provider shall be liable for delay or failure to perform in whole or in part any of their respective obligations and responsibilities lack or failure of raw materials, war, acts of God, hurricanes, fires, storms, accidents, and force majeure, government regulations or interference of any cause whatever beyond the concerned party's control;

Payment terms: 30 days after complete delivery

Note: •Quoted price/s must be VAT inclusive.

•Supplier must have a Land Bank of the Phil. Account.

•Supplier must submit a sealed quotation.

•Sealed quotation must be submitted together with the following requirements:

Company Profile, DTI/SEC Registration, Business/Mayor's Permit, BIR Registration, and PhilGEPs Certificate of Membership

Signature over Printed Name

Contact Numbers (Landline and/or Cellphone Nos.)/E-mail address

TERMS AND CONDITIONS

1. Bidders shall provide correct and accurate information required in this form.
2. Price quotations/s must be valid for a period of Thirty (30) calendar days from the date of submission.
3. Price quotations, to be denominated in Philippine peso shall include all taxes.
4. Quotations exceeding the Approved Budget for the Contract shall be rejected.
5. Award of contract shall be made to the lowest quotation (for goods and infrastructure) or, the highest rated offer (for consulting services) which complies with the minimum technical specifications and other terms and conditions stated herein.
6. Any interlineations, erasures or overwriting shall be valid only if they are signed or initialed by you or any of your duly authorized representative/s. _____
7. The items shall be delivered within _____ working days from receipt of Purchase/Job Order.
8. The CDA-CO shall have the right to inspect and/or to test the goods
9. Submit your sealed quotation by mail or through your messenger addressed to the Cooperative Development Authority, 827 Aurora Blvd., Brgy. Immaculate Concepcion, Quezon City.
10. The Cooperative Development Authority reserves the right to accept or reject any or all quotations, waive any informality or technicality therein and award to any firm whose proposal is deemed most advantageous to the government.