Bids and Awards Committee

Republic of the Philippines
Professional Regulation Commission
P. Paredes St., Sampaloc, Metro Manila
Facsimile: 5-310-0037 / email: bac@prc.gov.ph

REGULAR MEMBERS:

ARISTOGERSON T. GESMUNDO
Chairman

OMAIMAH E. GANDAMRA
Vice-Chairperson

WILMA T. UNANA
Member

CRISANTO L. DECENA
Member

CARLA ANGELINE B. UJANO
Member

ALTERNATE MEMBERS:

MARIA LIZA M. HERNANDEZ
Vice-Chairperson

ARJAY R. ROSALES
Member

HENRIETTA P. NARVAEZ
Member

PROVISIONAL MEMBERS:

TEODORO V. MENDOZA II
Provisional Member, Non-IT Projects

RICHARD M. ARANIEGO
Provisional Member, IT Projects

SECRETARIAT:

KAREN M. MAGSALIN
Secretary

MARGIERY D. DULIN
Member

MARIA ENRICA D. JUBAY
Member

CHRISTOPHER A. MAYO
Member

ELIEZER C. LEYCO
Member

LIEZEL F. BURAGA
Member

JOEL P. IGNACIO
Member

Section VII. Technical Specifications

No	Item	Specification	Statement of Compliance
1 Lot	1 unit	**SUPPLY, DELIVERY, INSTALLATION, AND CONFIGURATION OF ONE (1) UNIT LOAD BALANCER (APPLICATION DELIVERY CONTROLLER)** **1. General solution requirements** **1.1. Product Architecture** **1.1.1.** The solution should support different deployment modes: One-Arm mode, Transparent, Router, high availability (HA A/P). **1.2. Technical Details** **1.2.1.** Solution should support at least 8 interfaces and up to 1GbEinterfaces (4 GE RJ45, 4 GE SFP) **1.2.2.** Solution should support from 500Mbps and up to at least 8Gbps L4/L7 throughput **1.2.3.** Solution should support at least 200,000 L4 connections per second **1.2.4.** Solution should support at least 8M L4 concurrent connections **1.2.5.** 1 RU form factor appliance options available **1.2.6.** Appliance options should have at least 120GB of local storage **1.2.7.** Solution should also be available as a virtualized appliance. **1.2.7.1.** Solution should support: VMware, Hyper-V, KVM, Citrix Xen; Server and Open-Source Xen. **1.2.8.** Solution should be available from Amazon Cloud (AWS), Microsoft Azure, Oracle (OCI) and Google Cloud (GCP) **1.2.9.** The virtualized solution should have the same features as the hardware appliance **1.2.10.** Solution should also support with HSM (SafeNet Integration) **1.2.11.** Solution should support integration with sandbox solution to scan file attachments for known and unknown threats **1.3. Solution should support Virtual Domains (VDOMs) with configuration and performance limit for each VDOM**	

REGULAR MEMBERS:

ARISTOGERSON T. GESMUNDO
Chairman

OMAIMAH E. GANDAMRA
Vice-Chairperson

WILMA T. UNANA
Member

CRISANTO L. DECENA
Member

CARLA ANGELINE B. UJANO
Member

ALTERNATE MEMBERS:

MARIA LIZA M. HERNANDEZ
Vice-Chairperson

ARJAY R. ROSALES
Member

HENRIETTA P. NARVAEZ
Member

PROVISIONAL MEMBERS:

TEODORO V. MENDOZA II
Provisional Member, Non-IT Projects

RICHARD M. ARANIEGO
Provisional Member, IT Projects

SECRETARIAT:

KAREN M. MAGSALIN
Secretary

MARGIERY D. DULIN
Member

MARIA ENRICA D. JUBAY
Member

CHRISTOPHER A. MAYO
Member

ELIEZER C. LEYCO
Member

LIEZEL F. BURAGA
Member

JOEL P. IGNACIO
Member

1.4. Management

1.4.1. Solution should support the following access:

1.4.1.1. SSH, WebUI (HTTP/S), Restful API, Console

1.4.2. Solution should support Access Control:

1.4.2.1. Read-write, Read only, Password policy (replace old password, minimum password length), Authentication using remote LDAP or RADIUS

1.5. Backup and restore configuration

1.5.1. Solution should support backup procedure to save a copy of your system configuration.

1.5.1.1. Backup - backup the current configuration.

1.5.1.2. Restore - restore a previous configuration.

1.5.1.3. Storage of backup can be Local PC/Server or local ADC

1.6. High Availability

1.6.1. Solution should be available in Active/Passive failover and Active/Active

1.6.2. Full configuration and session sync

1.6.3. A centralized management solution should NOT be needed when using a cluster of units

1.6.4. Units should synchronize the following objects: ruleset, configured policies, objects.

1.7. Dynamic Routing/Services

1.7.1. Support the following routing protocols:

1.7.1.1. BGP (Border Gateway Protocol)

1.7.1.2. OSPF (Open Shortest Path First)

1.7.1.3. Route health injection (RHI) - allows for advertising routes to virtual server IP addresses based on the health status of the corresponding service via OSPF or BGP.

1.8. QoS (Quality of Service)

1.8.1. Control network bandwidth usage to fit business need and improve user experience. Traffic is classified to different priority queues with bandwidth allocated. Dispatcher may buffer (limited by buffer space) outbound and dropped for inbound packets when reach bandwidth limit.

REGULAR MEMBERS:

ARISTOGERSON T. GESMUNDO
Chairman

OMAIMAH E. GANDAMRA
Vice-Chairperson

WILMA T. UNANA
Member

CRISANTO L. DECENA
Member

CARLA ANGELINE B. UJANO
Member

ALTERNATE MEMBERS:

MARIA LIZA M. HERNANDEZ
Vice-Chairperson

ARJAY R. ROSALES
Member

HENRIETTA P. NARVAEZ
Member

PROVISIONAL MEMBERS:

TEODORO V. MENDOZA II
Provisional Member, Non-IT Projects

RICHARD M. ARANIEGO
Provisional Member, IT Projects

SECRETARIAT:

KAREN M. MAGSALIN
Secretary

MARGIERY D. DULIN
Member

MARIA ENRICA D. JUBAY
Member

CHRISTOPHER A. MAYO
Member

ELIEZER C. LEYCO
Member

LIEZEL F. BURAGA
Member

JOEL P. IGNACIO
Member

		1.9. VDOMs (Virtual Domains) **1.9.1.** Solution should support virtual domains (VDOMs). A virtual domain **1.9.2.** (VDOM) is a complete ADC instance that runs on the ADC platform. **1.9.3.** The VDOM feature supports multi-tenant deployments. **1.10. ADC allows you to create and impose custom policies or restrictions on each virtual domain you have added. For each virtual domain, you can configure the maximum range for its Dynamic Resources and Static Resources** **2. Server Load Balancing & Application Optimization Features** **2.1. Application/Protocol support** **2.1.1.** Solution should support both IPv4 and IPv6 **2.1.2.** Solution should support HTTP/1.0, HTTP/1.1 and HTTP/2 **2.1.2.1.** Support service delivery and security on both HTTP protocols **2.1.2.2.** Support HTTP/2 client to HTTP/1.1 backend side deployment **2.1.3.** Supported protocols: **2.1.3.1.** HTTP, HTTPS, DNS, SIP, RTSP, RTMP, TCP, UDP, RADIUS, IP, FTP, RDP, MySQL, MSSQL **2.2. Application Health Check** **2.2.1.** The solution should be capable of implementing health-checks for your application servers for the purpose of load balancing pool removal and administrator notification. **2.2.2.** The solution should be capable of supporting at least the following health Check protocols: **2.2.2.1.** ICMP,TCP Echo, TCP, HTTP, HTTPS, DNS **2.3. Application Load balancing, Persistency, Content rewrite/routing and NAT** **2.3.1.** Load Balancing algorithms **2.3.1.1.** Round Robin **2.3.1.2.** Faster Response **2.3.1.3.** Least Connection **2.3.1.4.** Weighted Round-Robin **2.3.2.** Persistency features: **2.3.2.1.** Source-IP **2.3.2.2.** Source IP / Port Hash	

REGULAR MEMBERS:

ARISTOGERSON T. GESMUNDO
Chairman

OMAIMAH E. GANDAMRA
Vice-Chairperson

WILMA T. UNANA
Member

CRISANTO L. DECENA
Member

CARLA ANGELINE B. UJANO
Member

ALTERNATE MEMBERS:

MARIA LIZA M. HERNANDEZ
Vice-Chairperson

ARJAY R. ROSALES
Member

HENRIETTA P. NARVAEZ
Member

PROVISIONAL MEMBERS:

TEODORO V. MENDOZA II
Provisional Member, Non-IT Projects

RICHARD M. ARANIEGO
Provisional Member, IT Projects

SECRETARIAT:

KAREN M. MAGSALIN
Secretary

MARGIERY D. DULIN
Member

MARIA ENRICA D. JUBAY
Member

CHRISTOPHER A. MAYO
Member

ELIEZER C. LEYCO
Member

LIEZEL F. BURAGA
Member

JOEL P. IGNACIO
Member

		2.3.2.3. HTTP Header **2.3.2.4.** HTTP Request Hash **2.3.2.5.** Hash Cookie **2.3.2.6.** SSL Session ID **2.3.2.7.** RADIUS Attribute **2.3.2.8.** Insert Cookie **2.3.2.9.** Rewrite Cookie **2.3.2.10.** Embedded Cookie **2.3.3.** L7 Content Rewrite and Content Routing **2.3.3.1.** Content Rewrite: **2.3.3.1.1.** Rewrite HTTP Header (Header and URL) **2.3.3.1.2.** Insert/delete HTTP Header **2.3.3.1.3.** Redirect according to match condition **2.3.3.1.4.** Send 403 forbidden **2.3.3.2.** Content Routing according to String or Regex: **2.3.3.2.1.** HTTP Host Header **2.3.3.2.2.** HTTP Referrer Header **2.3.3.2.3.** HTTP Request URL **2.3.3.2.4.** SNI **2.3.3.2.5.** Source IP Address **2.3.4.** The solution should support NAT **2.3.4.1.** Source NAT (change source IP) **2.3.4.2.** 1:1 NAT **2.3.4.3.** DNAT (change destination IP) **2.3.4.4.** Full NAT (change source & destination IP) **2.3.4.5.** NAT46 **2.3.4.6.** NAT64 **2.4. Application Optimization** **2.4.1.** Solution should support web site acceleration functions **2.4.1.1.** Dynamic and static Caching **2.4.1.1.1.** Provide full caching for your application **2.4.1.1.2.** HTTP responses with status codes 200, 203, 300, 301, 400 can be cached. **2.4.1.2.** Compression/decompression **2.4.1.2.1.** application/JavaScript **2.4.1.2.2.** application/x-JavaScript **2.4.1.2.3.** application/xml **2.4.1.2.4.** text/CSS **2.4.1.2.5.** text/html **2.4.1.2.6.** text/JavaScript **2.4.1.2.7.** text/plain **2.4.1.2.8.** text/xml **2.5. SSL/TLS** **2.5.1.** SSL Offloading **2.5.1.1.** ADC can forward data	

REGULAR MEMBERS:

ARISTOGERSON T. GESMUNDO
Chairman

OMAIMAH E. GANDAMRA
Vice-Chairperson

WILMA T. UNANA
Member

CRISANTO L. DECENA
Member

CARLA ANGELINE B. UJANO
Member

ALTERNATE MEMBERS:

MARIA LIZA M. HERNANDEZ
Vice-Chairperson

ARJAY R. ROSALES
Member

HENRIETTA P. NARVAEZ
Member

PROVISIONAL MEMBERS:

TEODORO V. MENDOZA II
Provisional Member, Non-IT Projects

RICHARD M. ARANIEGO
Provisional Member, IT Projects

SECRETARIAT:

KAREN M. MAGSALIN
Secretary

MARGIERY D. DULIN
Member

MARIA ENRICA D. JUBAY
Member

CHRISTOPHER A. MAYO
Member

ELIEZER C. LEYCO
Member

LIEZEL F. BURAGA
Member

JOEL P. IGNACIO
Member

		unencrypted to the servers, and the servers can maximize performance because they are processing. **2.5.1.2.** HTTP and not HTTPS transactions. **2.5.1.3.** Client SSL –ADC can terminate client requests sent via the SSL protocol and pass it to real server in HTTP. **2.5.1.4.** Server SSL –ADC can re-encrypt HTTP traffic to real server (end to end SSL) **2.5.2.** SSL Visibility **2.5.2.1.** ADC supports mirroring packets (HTTPS/TCPS) to specified network interfaces. When the feature is enabled, SSL traffic will be mirrored to the specified ports by the virtual server after it has been decrypted **2.5.3.** SSL Forward-Proxy **2.5.3.1.** ADC support SSL Forward-Proxy for client traffic. When SSL forward proxy is enabled, ADC becomes a proxy to both sides of the connection. The server certificate and its private key used to negotiate the SSL connection with the client are dynamically derived from the certificate presented by the real server. **2.5.4.** The ADC system supports all of the TLS/SSL methods commonly used by HTTPS servers, including: **2.5.4.1.** Server name indication (SNI) **2.5.4.2.** Local certificate store **2.5.4.3.** Intermediate CAs store **2.5.4.4.** Certificate Authorities (CAs) store **2.5.4.5.** OCSP/OCSP stapling **2.5.4.6.** CRL **2.5.4.7.** All digital certificates of RSA and ECDSA key types – whether they are local, remote, intermediate, or CA root certificates. **2.5.4.8.** Client certificate forwarding. **2.5.4.9.** SNI forwarding. **2.5.5.** Certificates Support: **2.5.5.1.** Local Certificates/intermediate Certificates **2.5.5.2.** Local Certificate Groups/Intermediate CA Groups **2.5.5.3.** CA/CRL/OCSP Signing	

REGULAR MEMBERS:

ARISTOGERSON T. GESMUNDO
Chairman

OMAIMAH E. GANDAMRA
Vice-Chairperson

WILMA T. UNANA
Member

CRISANTO L. DECENA
Member

CARLA ANGELINE B. UJANO
Member

ALTERNATE MEMBERS:

MARIA LIZA M. HERNANDEZ
Vice-Chairperson

ARJAY R. ROSALES
Member

HENRIETTA P. NARVAEZ
Member

PROVISIONAL MEMBERS:

TEODORO V. MENDOZA II
Provisional Member, Non-IT Projects

RICHARD M. ARANIEGO
Provisional Member, IT Projects

SECRETARIAT:

KAREN M. MAGSALIN
Secretary

MARGIERY D. DULIN
Member

MARIA ENRICA D. JUBAY
Member

CHRISTOPHER A. MAYO
Member

ELIEZER C. LEYCO
Member

LIEZEL F. BURAGA
Member

JOEL P. IGNACIO
Member

		Certificates **2.5.6.** SSL/TLS version supported: SSLv3, TLSv1.0, TLSv1.1, TLSv1.2, TLSv1.3 **3. Web Application Firewall Features** A web application firewall (WAF) is a security policy enforcement point positioned between a client endpoint and a web application. The primary purpose is to prevent attacks against the web servers. ADC should be able to provide a full Web Application Firewall solution with the following features: **3.1. Negative security model (Attack Signatures)** **3.1.1.** The solution should offer a negative security model **3.1.2.** The signature database should be automatically updated **3.1.3.** Default policies should be available in various classifications, Alert Only, Medium Security, High Security **3.1.4.** Signatures should be grouped in logical, searchable dictionaries. The list should at least contain: **3.1.4.1.** Cross Site Scripting **3.1.4.2.** SQL Injection **3.1.4.3.** Generic Attacks **3.1.4.4.** Known Exploits **3.1.4.5.** Application Attacks **3.2. Web Vulnerability Scanner (WVS)** **3.3. XML, JSON and SOAP Validation** **3.4. Data leak prevention** **3.5. HTTP Compliance validation** **3.6. Anti-Web Defacement** **3.7. Brute Force Attack Detection** **4. Global Load Balancing Features** **4.1. The global load balancing (GLB) feature is a DNS-based solution that enables to deploy redundant resources around the globe that can be leveraged to keep business online when a local area deployment experiences unexpected spikes or downtime. The ADC system should be able to support below features:** **4.1.1.** Virtual server health check- availability is determined by real-time connectivity checking. **4.1.2.** Dynamic proximity - proximity is determined by application response time (RTT probes), least connections, or byte-per-second. **4.1.3.** Weighted round robin - if proximity algorithms are not configured or not applicable, available virtual servers are	

REGULAR MEMBERS:

ARISTOGERSON T. GESMUNDO
Chairman

OMAIMAH E. GANDAMRA
Vice-Chairperson

WILMA T. UNANA
Member

CRISANTO L. DECENA
Member

CARLA ANGELINE B. UJANO
Member

ALTERNATE MEMBERS:

MARIA LIZA M. HERNANDEZ
Vice-Chairperson

ARJAY R. ROSALES
Member

HENRIETTA P. NARVAEZ
Member

PROVISIONAL MEMBERS:

TEODORO V. MENDOZA II
Provisional Member, Non-IT Projects

RICHARD M. ARANIEGO
Provisional Member, IT Projects

SECRETARIAT:

KAREN M. MAGSALIN
Secretary

MARGIERY D. DULIN
Member

MARIA ENRICA D. JUBAY
Member

CHRISTOPHER A. MAYO
Member

ELIEZER C. LEYCO
Member

LIEZEL F. BURAGA
Member

JOEL P. IGNACIO
Member

listed in order based on a simple load balancing algorithm.

4.1.4. Full DNS Function Support - CANME, A record, AAAA record, MX record, CNAME record, NS record, TXT record, SRV record.

5. User Authentication

5.1. Authentication Methods

5.1.1. Solution should support multiple client authentication method

5.1.1.1. Basic Authentication

5.1.1.2. Form Based Authentication

5.1.1.3. Client Certificate Authentication

5.1.1.4. SAML Authentication

5.1.2. Solution should support Authentication Delegation

5.1.2.1. Kerberos Authentication, including multiple server option

5.1.2.2. RADIUS Authentication

5.1.2.3. LDAP/AD Authentication

5.1.3. Solution should support Single Sign On (SSO)

5.1.3.1. SAML 2.0 Authentication

5.1.3.1.1. Provides support for service provider (SP) and Identity Provider (IDP) Metadata

5.1.3.1.2. Provides single sign-on (SSO) experience for all virtual server resources linked with the user log-in

5.1.3.1.3. Solution should function as SP, ADC should support FortiAuthenticator

5.1.4. Solution should support Two Factor Authentication, for strong application access, with FortiToken and Google Authenticator.

6. Security Features

6.1. Anti-DDoS Protection

6.1.1. The solution should offer Layer 7 DDoS capabilities to stop any service disruption

6.2. L4 Firewall

6.2.1. A firewall policy is a filter that allows or denies traffic based on a: source address, destination address, and service. By default, firewall policy rules are stateful: if client-to-server traffic is allowed, the session is maintained in a state table, and the response traffic is allowed.

REGULAR MEMBERS:

ARISTOGERSON T. GESMUNDO
Chairman

OMAIMAH E. GANDAMRA
Vice-Chairperson

WILMA T. UNANA
Member

CRISANTO L. DECENA
Member

CARLA ANGELINE B. UJANO
Member

ALTERNATE MEMBERS:

MARIA LIZA M. HERNANDEZ
Vice-Chairperson

ARJAY R. ROSALES
Member

HENRIETTA P. NARVAEZ
Member

PROVISIONAL MEMBERS:

TEODORO V. MENDOZA II
Provisional Member, Non-IT Projects

RICHARD M. ARANIEGO
Provisional Member, IT Projects

SECRETARIAT:

KAREN M. MAGSALIN
Secretary

MARGIERY D. DULIN
Member

MARIA ENRICA D. JUBAY
Member

CHRISTOPHER A. MAYO
Member

ELIEZER C. LEYCO
Member

LIEZEL F. BURAGA
Member

JOEL P. IGNACIO
Member

		6.3. Intrusion Prevention System (Subscription-based) **6.3.1.** Intrusion Prevention Service should provide the latest defenses against stealthy network-level threats. **6.4. Anti-Virus and Malware solution (Subscription-based)** **6.4.1.** The solution should offer an on-board Anti-Virus solution **6.4.2.** The AV database should be automatically updated **6.4.3.** The AV solution should NOT introduce additional software or hardware deployments nor 3rd-party integration requirements. **6.4.4.** Solution should tightly integrate with Sandboxing solution for file upload protection and learn observed malicious content from it. **6.5. IP Reputation (Subscription-based)** **6.5.1.** Solution should be capable of detecting and distinguishing two sets of Bots from the Internet: **6.5.1.1.** Known search engines **6.5.1.2.** Bad robots (scanners, crawlers, spiders) **6.6. Geo IP Protection (Subscription-based)** **6.6.1.** Geo IP service provides a database that maps IP addresses to countries, satellite providers, and anonymous proxies. The database is updated periodically. **7. Link Load Balancing Features** **7.1. Provides WAN link redundancy and failover, multi-homing of multiple ISPs. Policy/Intelligent routing reduces WAN cost, improves user experience, and optimizes WAN usage.** **7.1.1.** Supported LB Methods - Weighted Round Robin, Least Connections, Least New Connections per Second **7.1.2.** Supported Health Check Types - same HC database as SLB has. **7.1.3.** Supported Persistence Methods - source-destination pair, Source destination address, Source address, Destination address **7.1.4.** Policy Based Routing (eRoute) - route traffic based on source/target IP, port, protocol, priority to different ISPs, failover	

REGULAR MEMBERS:

ARISTOGERSON T. GESMUNDO
Chairman

OMAIMAH E. GANDAMRA
Vice-Chairperson

WILMA T. UNANA
Member

CRISANTO L. DECENA
Member

CARLA ANGELINE B. UJANO
Member

ALTERNATE MEMBERS:

MARIA LIZA M. HERNANDEZ
Vice-Chairperson

ARJAY R. ROSALES
Member

HENRIETTA P. NARVAEZ
Member

PROVISIONAL MEMBERS:

TEODORO V. MENDOZA II
Provisional Member, Non-IT Projects

RICHARD M. ARANIEGO
Provisional Member, IT Projects

SECRETARIAT:

KAREN M. MAGSALIN
Secretary

MARGIERY D. DULIN
Member

MARIA ENRICA D. JUBAY
Member

CHRISTOPHER A. MAYO
Member

ELIEZER C. LEYCO
Member

LIEZEL F. BURAGA
Member

JOEL P. IGNACIO
Member

8. Monitoring and Reporting

8.1. Monitoring

8.1.1. The solution should have a dashboard showing system resources

8.1.2. The solution should have a dashboard showing real time Traffic Throughput, Connection, Attack and system information

8.1.3. The solutions should have drill down facility on at least the following info:

8.1.3.1. Server Load Balancing

8.1.3.1.1. End to End Timing (default)
8.1.3.1.2. Throughput
8.1.3.1.3. Concurrent Connections
8.1.3.1.4. Connections per Second
8.1.3.1.5. Request per Second

8.1.3.2. Web Application Firewall

8.1.3.2.1. Live Threat map
8.1.3.2.2. Attack info
8.1.3.2.3. Attack Type

8.2. Logging and Reporting

8.2.1. The solution should be able to locally store event (audit) information.

8.2.2. The solution should be able to locally store alert information.

8.2.3. The solution should be able to locally store traffic information.

8.2.4. The solution should be able to send all 3 log types above to a centralized logging system supplied by the vendor (optional)

8.2.5. The solution should be able to send all log types above to an external syslog server.

8.3. Data Analytics

8.3.1. The solution should have a dashboard for data analytics in which you can see at least the following information:

8.3.1.1. Server Load Balance:

8.3.1.1.1. Top Source IP
8.3.1.1.2. Top Destination IP
8.3.1.1.3. Top Session

8.3.1.2. Web Application Firewall:

8.3.1.2.1. Top Attack Type for All
8.3.1.2.2. Top Attack Type by VS for All
8.3.1.2.3. Top VS for DDoS

9. Compliance:

9.1. Solution should protect against common threats such as those identified in the OWASP top 10

REGULAR MEMBERS:

ARISTOGERSON T. GESMUNDO
Chairman

OMAIMAH E. GANDAMRA
Vice-Chairperson

WILMA T. UNANA
Member

CRISANTO L. DECENA
Member

CARLA ANGELINE B. UJANO
Member

ALTERNATE MEMBERS:

MARIA LIZA M. HERNANDEZ
Vice-Chairperson

ARJAY R. ROSALES
Member

HENRIETTA P. NARVAEZ
Member

PROVISIONAL MEMBERS:

TEODORO V. MENDOZA II
Provisional Member, Non-IT Projects

RICHARD M. ARANIEGO
Provisional Member, IT Projects

SECRETARIAT:

KAREN M. MAGSALIN
Secretary

MARGIERY D. DULIN
Member

MARIA ENRICA D. JUBAY
Member

CHRISTOPHER A. MAYO
Member

ELIEZER C. LEYCO
Member

LIEZEL F. BURAGA
Member

JOEL P. IGNACIO
Member

		10. Certification: **10.1.** The Prospective bidder must be an **ISO/IEC 27001:2013** Certified Company. Must submit valid and updated certificate. **11. Scope of Work** **11.1.** Supply, Delivery, Installation and Configuration of 1-unit Load Balancer (Application Delivery Controller) to the PRC Central Office **11.2.** With Free One (1) year Preventive Maintenance. **11.3.** Hands-on Training for 3 Personnel **12. Local Onsite Support** **12.1.** 1 yr. Limited Onsite Technical Support – 8x5 Onsite Assistance with 4 hrs. Response time during Regular Business Hours (Monday to Friday excluding Holidays, 9AM to 6PM).	

1. Compliance with the statements must be supported by evidence in a Bidders Bid and cross-referenced to that evidence. Evidence shall be in the form of manufacturer's un-amended sales literature, unconditional statements of specification and compliance issued by the manufacturer, samples, independent test data etc., as appropriate.

2. A statement that is not supported by evidence or is subsequently found to be contradicted by the evidence presented will render the Bid under evaluation liable for rejection.

3. A statement either in the Bidders statement of compliance or the supporting evidence that is found to be false either during Bid evaluation, post-qualification or the execution of the Contract may be regarded as fraudulent and render the Bidder or supplier liable for prosecution subject to the provisions of **ITB** Clause 3.1 (a) (ii) and/or **GCC** Clause 2.1 (a) (ii).

ACKNOWLEDGMENT AND COMPLIANCE WITH THE TERMS OF REFERENCE FOR THE PROCUREMENT AND DELIVERY OF LOAD BALANCER (APPLICATION DELIVERY CONTROLLER)

_____
SIGNATURE OVER PRINTED NAME
OF AUTHORIZED REPRESENTATIVE,
DESIGNATION AND PRINTED NAME OF COMPANY