TERMS OF REFERENCE
SUPPLY, DELIVERY, INSTALLATION AND CONFIGURATION OF SERVER LOAD BALANCER

1. BACKGROUND

1.1 Project Background and Objectives

The Department of Justice (DOJ) of the Republic of the Philippines are rolling out several applications which will use the Public Internet as its transport medium. This project seeks to ensure a continuous, reliable, and secure connection between the client and the servers which dispenses these applications.

1.2 Current Information Security Posture

The DOJ has several Security Systems in Place. Active Directory, Firewalls, Endpoint Security, are deployed all throughout the Main Office and NCR offices. There are also existing security policies in place.

1.3 About the DOJ

The Department of Justice (DOJ) derives its mandate primarily from the Administrative Code of 1987 (Executive Order No. 292). It carries out this mandate through the Department Proper and the Department's attached agencies under the direct control and supervision of the Secretary of Justice.

Under Executive Order (EO) 292, the DOJ is the government's principal law agency. As such, the DOJ serves as the government's prosecution arm and administers the government's criminal justice system by investigating crimes, prosecuting offenders and overseeing the correctional system.

The DOJ, through its offices and constituent/attached agencies, is also the government's legal counsel and representative in litigations and proceedings requiring the services of a lawyer; implements the Philippines' laws on the admission and stay of aliens within its territory; and provides free legal services to indigent and other qualified citizens.

1.4 The Requirement

The DOJ is soliciting proposals for Server Load Balancer

2. APPROVED BUDGET FOR THE CONTRACT (ABC)

The Approved Budget for the Contract is Four Million Nine Hundred Thousand Pesos (4, 900,000.00) Inclusive of Value-Added Tax (V.A.T.) and all other applicable government taxes.

3. TIMELINE, OUTCOME AND PERFORMANCE STANDARDS

3.1 Terms of Engagement

The Terms of Engagement will be for Three (3) Years, with expected full Operational Capability at within Forty-Five (45) Calendar Days after awarding of contract.

3.2 Project Management

The Contractor will apply Globally Accepted Best Practices and Standards for Project Management.

3.2.1 *Project Manager*
The Contractor will assignment of a dedicated Project Manager (PM) that will serve as the main Point-of-Contact (POC) during the Implementation of the Project.

3.2.2 *Project Plan*
The Project Manager will provide a comprehensive Project Plan detailing the tasks, timelines, resources, and milestones of the project.

3.2.3 *Weekly Reporting*
The Project Manager will provide a report and update DOJ and its appointed contact/s the status of the Implementation of the Project on a weekly basis.

3.3 Service Management

The Contractor will apply Globally Accepted Best Practices and Standards for Service Management.

3.3.1 *Service Delivery Manager*
The Contractor will assignment of a dedicated Service Delivery Manager (SDM) that will serve as the main Point-of-Contact (POC) during the Operational Stages (Business-as-Usual: BAU) of the Project.

3.3.2 *Project Plan*
The Service Delivery Manager will provide an Incident Response Program that will include an Escalation Protocol detailing the severity levels and contact details of the appropriate Support Personnel or Subject Matter Expert (SME).

3.3.3 *Weekly Reporting*
The Service Delivery Manager will provide a report and update DOJ and its appointed contact/s the status of the System, Current Incidents, and other pertinent information on a weekly basis.

4. CONTRACTORS QUALIFICATION

4.1 Business and Continuous Operation

The Contractor must be a company that has been continually operating for at least Five (5) years providing Systems Integration, Software Development, and Information Security Products and Services.

4.2 Project and Service Management Competency

The Contractor must have Project and Service Delivery Managers certified by Global and Industry Accepted Organizations.

4.3 Information Security Competency

The Contractor must have Certified Information Security Professionals and Engineers certified by the vendor or manufacturer, as well as other Global and Industry Accepted Organizations.

4.4 Required Documentation

The Contractor is required to submit the following documentation:

4.4.1 *Curriculum Vitae and Certification of Project and Service Delivery Manager*
Copy of Certificates and Curriculum Vitae of all Project Managers and Service Managers that will be assigned to the project.

4.4.2 *Curriculum Vitae and Certification of Information Security Professionals*
Copy of Certificates and Curriculum Vitae of all Information Security Professionals and Engineers that will be assigned to the project.

4.4.3 *Non-Disclosure Agreement (NDA)*
A Non-Disclosure Agreement attached and marked as Appendix "B" should be signed and submitted to DOJ.

5. SERVICE REQUIREMENTS

5.1. Core Requirements
This project shall include as a standard, the following:

5.1.1 Provisioning*, management, monitoring, deployment, integration, installation and support, and all services necessary to fulfil and operationalize the equipment.*

5.1.2 *24x7 Availability, Monitoring, Notification, and Technical Support.*

5.1.3 *Management, Monitoring, and Reporting Dashboards.*

5.1.4 *Operations and Management Certification Training for Five (5) DOJ personnel*

5.2 Load Balancer Technical Specifications

The Load Balancer Appliance should support at a minimum the following specifications:

#	Minimum Specifications
	Appliance
5.2.1	ASIC based, high performance purpose built Hardware
5.2.2	48 GB DDR4 RAM supporting load balancing features and other features, Min. 400G SSD hard drive
5.2.3	Minimum 6 triple speed 10/100/1000 MBps copper ports and 2*10G SFP+ ports.
5.2.4	Minimum 1.5M L7 HTTP requests/sec

5.2.5	Multi-tenancy capability with CPU, Memory, Firmware, SSL, independent reboot for each instance
5.2.6	Redundant Power Supply
5.2.7	Minimum 30 GBps of L7 throughput, Minimum 50Gps L4 throughput
5.2.8	Minimum 5 years' support and maintenance from end of sale/life
5.2.9	Minimum 5 GBps compression throughput
5.2.10	Minimum 100 SSL VPN concurrent users
5.2.11	Support for ADC, SSL VPN
5.2.12	Minimum 125K concurrent connections scalable to 10M
Load Balancing	
5.2.13	Supports layer 2 to layer 7 load balancing
5.2.14	Supports server load balancing algorithms i.e. round robin, weighted round robin, least connection, Persistent IP, Hash IP, Hash Cookie, consistent hash IP, shortest response, proximity, SNMP, SIP session ID, hash header and others
5.2.15	Supports one arm, reverse and transparent proxy mode deployment scenarios and should support nested layer7 and l4 policies
5.2.16	Supports server persistency based on source IP and destination IP, http header, URL, cookie and SSL ID
5.2.17	Support for HTTP/SSL offloading
5.2.18	Support for multi-port, scripted and custom health check with content verification
5.2.19	Support for Application & server health checks for well-known protocols i.e. ARP, ICMP, TCP, DNS, RADIUS, HTTP/HTTPS, RTSP and others
5.2.20	Support for layer4 and layer 7 load balancing for HTTP/HTTPS, FTP/FTPS, SIP, RTSP , RDP, TCP, TCPS and UDP protocols
5.2.21	Support for graceful shut down of real services
Failover and Clustering	
5.2.22	Support for high-availability and N+1 clustering
5.2.23	Support for Stateful session failover with Active-active & active standby unit redundancy mode.
5.2.24	Support for multiple communication links for real time configuration synchronizations including HA group, gateway health check, decision rules, SSF sessions etc. and heartbeat information
5.2.25	Support for floating MAC address to avoid MAC table updates on the upstream routers/switches and to speed up the failover
5.2.26	Support for floating IP address and group for state full failover support.
5.2.27	Support for 256 floating IP address for a floating group
5.2.28	Support for failover decision/health check conditions.
5.2.29	Option to define customized rules for gateway health check - administrator should able to define a rule to inspect the status of the link between the unit and a gateway
Application and Security Acceleration	
5.2.30	Should support advance ACL's to protect against network based flooding attacks. Administrator should able to define ACL's rules based on connections per second (CPS) and concurrent connections (CC), cookie value.
5.2.31	Support for performance optimization using TCP connection multiplexing, TCP buffering and IEEE 802.3ad link aggregation
5.2.32	Support for TCP optimization options including windows scaling, timestamp & Selective Acknowledgement for enhanced TCP transmission speed
5.2.33	TCP optimization option configuration should be defined on per virtual service basis not globally
5.2.34	Support for real time Dynamic Web Content Compression to reduce server load
5.2.35	Support for selective compression for Text, HTML, XML, DOC, Java Scripts, CSS, PDF, PPT, and XLS Mime types.
5.2.36	Provision to define policy to skip compression for selected trouble URL (RegEx, Web Objects) for the specified Virtual
5.2.37	Provide Advanced high performance memory/packet based Web cache; fully integrated with HTTP/HTTPS
5.2.38	Support for customized cache rules including max object size, TTL objects, refresh time interval and others
5.2.39	Provide detailed cache access statistics based on IP or http hosts
5.2.40	Support cache refresh with CLI, XML-RPC input commands and "PURGE" request
5.2.41	Support for transparent, layer 7 proxy and triangular mode support
5.2.42	Support for L7 rule based application firewall to protect the internal applications within base license and should have IP reputation table by default

5.2.43	Provide security features like reverse proxy firewall, Synflood and dos attack protection features from the day of installation
5.2.44	Support for client & server TCP optimization by default
5.2.45	Capability to support application cache
5.2.46	Support for front end optimization functionalities like content layout, image optimization, style sheets and Java script optimization for mobile users
Management	
5.2.47	Provide extensive report and logging with built-in “tcpdump” like tool and log collecting functionality
5.2.48	Provide SSH CLI, Direct Console, SNMP, Single Console per Cluster with inbuilt reporting
5.2.49	Support for XML-RPC for integration with 3rd party management and monitoring
5.2.50	Provide detailed logs and graphs for real time and time based statistics
5.2.51	Support led warning and system log alert for failure of any of the power and CPU issues
5.2.52	Should have a centralized management tool
5.2.53	Support role based access control with different privilege levels for configuration management and monitoring of individual appliance or multiple appliances
5.2.54	Support for single window management for load balancer, site failover appliances, IPv6 gateway with integrated master console to generate and execute configuration scripts on one or more devices
5.2.55	Capability for a Central repository for active and archived configuration files for rapid provisioning of new appliances or rollback, Email notifications and alerts to avoid downtime and facilitate rapid recovery from faults
SSL Accelerator and IPV6 Gateway	
5.2.56	High performance SSL Accelerator with dedicated hardware and must integrate with existing IPv6 setup and appliance should be IPv6 compliant
5.2.57	Support for full ipv6 support
5.2.58	Compressive support for IPv6 functions to help with ipv4-to-ipv6 transition without business disruption and must provide support for dual stack, DNS64, NAT 64, DNS 46, NAT 46, IPv6 NAT
5.2.59	Support for various deployment modes for seamless integration including reverse proxy (IPv6 to IPv4, IPv4 to IPv6) and IPv6 to IPv6 transparent and reverse proxy mode
5.2.60	Provide comprehensive and reliable support for high availability and IPv6 VIP switchover and support for various IPv6 functions such as compression, caching, SSL acceleration & clustering
5.2.61	Provide Secure online application delivery using hardware-based high performance SSL acceleration with minimum of 3 GBps SSL throughput and minimum of 5,000 SSL on a 2048 bit key
5.2.62	Supports Certificate format as “OpenSSL/Apache, *.PEM", "MS IIS, *.PFX", and "Netscape
5.2.63	Contains additional hardware card to perform the SSL offloading / acceleration for 1024 and 2048 bit certificates
5.2.64	Supports Self generates CSR (Certificate Signing Request), self-signed Certificate and private key for specified host
Link Aggregation and Site Failover	
5.2.66	Provide a scalable, dedicated hardware platform to help ensure that all applications access must be provisioned through DR in event of service disruption at DC. The proposed solution must integrate with organization’s business critical applications and network devices such as application load balancer, IPv6 gateway
5.2.67	Support site selection feature to provide global load balancing features for disaster recovery and site redundancy
5.2.68	Support full DNS server to support all kind of DNS records including A, AAAA, MX, CNAME, PTR DNS records
5.2.69	Capable to evaluate round trip time (RTT), Persistence loss ratio (PLR) and hop count for dynamic proximity calculations
5.2.70	Support for global server load balancing algorithms including - Weighted round robin, Weighted Least Connections, Administrative Priority, Geography, Proximity, Global Connection Overflow (GCO), Global Least Connection (GLC), IP Overflow (IPO)
5.2.71	Support dynamic proximity rules instead of static proximity rules to direct the traffic to closest datacentre
5.2.72	Support for multiple internet links in Active-Active load balancing and active-standby failover mode
5.2.73	Support for inbound and outbound load balancing algorithms like round robin, Weighted round robin, shortest response, hash IP, target proximity and dynamic detect
5.2.74	Provide individual link health check based on physical port, ICMP Protocols, user defined l4 ports and destination path health checks

5.2.75	support persistency features including RTS (return to sender) and ip flow persistence.
5.2.76	provide comprehensive and reliable support for high availability and N+1 clustering based on Per VIP based Active-active & active standby unit redundancy mode
5.2.77	option to define customized rules for gateway health check - the administrator should able to define a rule to inspect the status of the link between the unit and a gateway
SIEM Compatibility	
5.2.78	The Solution should be able to provide logs which will are compatible to any Security Incident and Event Management (SIEM) System

7. WARRANTY AND SUPPORT

7.1 Three (3) years hardware warranty and technical support including all necessary subscription services and firmware upgrades

7.2 The winning bidder shall provide technical services and RMA support backed by a maintenance agreement specifying the terms and conditions of the warranty period and coverage. The maintenance agreement shall at least provide for the following services:

7.2.1 24x7 support availability by phone, email and onsite support
7.2.2 Unlimited access to the online knowledge base portal
7.2.3 Unlimited access to the online web support portal

8. TERMS AND CONDITIONDS

8.1 This TOR defines the coverage of DOJ's requirements for Load Balanceand does not constitute as a contract of any kind.
8.2 DOJ reserves the right to enter negotiations or discussions with other vendors or service providers.
8.3 DOJ reserves the right to reject all proposals as it may deem necessary.
8.4 Any information that will come out because of this tender shall be treated confidentially and may not be distributed to any party under any circumstances.
8.5 All information, diagrams and other details submitted by the bidder shall become property of DOJ.
8.6 Only officials and personalities that are legally authorized by the organization can sign whatever document pertaining to this tender.
8.7 Changes and other modifications to the submitted proposal may be allowed if it is prior to the stated deadline.
8.8 DOJ will not be obliged to proceed with any transaction related to this bid unless expressed in a written agreement between the two parties.

9. DEVIATION FROM REQUIREMENTS

The vendor will be allowed to deviate from the requirements of this TOR provided that said deviations will be equal or greater than those stipulated. Furthermore, any and all deviations should be listed and explained in detail within their proposal under a separate and dedicated provision.