Republic of the Philippines
Office of the Solicitor General
134 Amorsolo St., Legaspi Village, Makati City

Technical Working Group for
Information and Communications Technology

TERMS OF REFERENCE

SUBSCRIPTION OF MANAGED SD-WAN FOR OSG BRANCH OFFICES

Background:

The Office of the Solicitor General (OSG) requires a strong and secure network infrastructure to provide smooth communication between its central office and branch offices in multiple locations. With the growing demand for high-performance, scalable, and resilient network services, traditional WAN designs confront cost, complexity, and security concerns. To overcome these restrictions, OSG plans to adopt a Managed Software-Defined Wide Area Network (SD-WAN) solution that offers centralized control, optimal traffic management, and security features customized to government operations.

A Managed SD-WAN subscription will allow OSG to increase the reliability and efficiency of inter-branch communication, assuring consistent access to essential systems like the Case Management Information System (CMIS) and other cloud-based legal research tools. By utilizing a managed service model, OSG may delegate network management tasks to a reputable supplier while maintaining security regulations and performance standards. This initiative supports the government's digital transformation efforts to improve operational efficiency, minimize downtime, and boost cybersecurity across distant offices.

Objective:

The main objective of this Terms of Reference (TOR) is to secure a Managed SD-WAN Subscription that guarantees secure, optimized, and high-availability network connectivity for OSG branch offices. To ensure that critical applications and services are accessible without interruption, the solution must offer real-time network monitoring, automated failover, and dynamic traffic routing. Furthermore, to reduce the operational overhead for OSG's IT team, the service provider must provide end-to-end administration, which encompasses deployment, maintenance, and performance analytics.

Additionally, the objectives of this TOR are to improve network security by incorporating advanced threat protection, zero-trust access controls, and integrated encryption to protect sensitive legal data that is transmitted between offices. The SD-WAN solution that is chosen must be scalable to accommodate future expansions and adhere to government cybersecurity standards and industry best practices. The project's ultimate objective is to enhance OSG's wide area networking capabilities, thereby guaranteeing a more cost-effective, resilient, and agile delivery of legal services across the country.

==========

Terms:

1. *Scope.* – Supply and delivery of Subscription of Managed SD-WAN for OSG Branch Offices.

2. *ABC.* - The Approved Budget for the Contract (ABC) is **Four Million and Four Hundred Thousand Pesos (₱4,400,000.00) for twelve (12) months,** inclusive of all government taxes, charges, and other standard fees.

ICT SUBSCRIPTION			
ITEM	**QTY**	**UNIT COST**	**TOTAL**
Managed SD-WAN for OSG Branch Offices The solution must include the following: • Secured SD-WAN Platform for OSG Data Center Colocation • Secured SD-WAN Platform for the main office and remote Offices • Virtual Central Management Platform	**1**	4,400,000.00	4,400,000.00
		TOTAL	**₱ 4,400,000.00**

3. *Warranties and Schedule of Payment.* - To guarantee the performance by the winning bidder of its obligations under the contract, it shall post a performance security before the signing of the contract. The performance security shall be in an amount not less than the required percentage of the total contract price in any of the following forms and in accordance with the following schedule:

Form of Performance Security	Amount of Performance Security (Not less than the required % of the Total Contract Price)	Statement of Compliance
a) Cash or cashier's/ manager's check issued by a Universal of Commercial Bank.	**5%**	

b) Bank draft/ guarantee or irrevocable letter of credit issued by a Universal or Commercial Bank; *however,* it shall be confirmed or authenticated by a Universal or Commercial Bank if issued by a foreign bank.	**5%**	
c) Surety bond, callable upon demand, issued by a surety or insurance company duly certified by the Insurance Commission as authorized to issue such security.	**30%**	
TERMS OF PAYMENT		**Statement of Compliance**
Supplier agrees to be paid based on a billing scheme as follows:		
• Within thirty (30) days from completion of the delivery and issuance of the Inspection and Acceptance Report by the OSG and submission of all other required documents - 95% of the contract price. • One (1) year from the issuance of the Inspection and Acceptance Report by the OSG - 5% of the contract price. Any non-compliance with the technical support provisions or the requirements outlined in the Terms of Reference will result in the automatic forfeiture of the 5% Warranty Deposit.		

All bid prices shall be considered as fixed prices and therefore not subject to price escalation during contract implementation.

4. *Qualifications of the Supplier*:

a) The bidder must have completed, within the last three years from the date of submission and receipt of at least one (1) single contract of a similar nature, amounting to at least twenty-five percent (25%) of the ABC.

For this purpose, a similar contract shall refer to the procurement contract for any ICT security solution and or network and wireless LAN.

b) The ensure the maturity of the solution it must have the following certifications:

- ISO 9001 Quality Management System
- ISO/IEC 27001 Information Security Management System
- ISO 27701 Privacy Information Management System
- ISO/IEC 20000-1 Information Technology Service Management System
- ISO 29151 Information Security of Personally Identifiable Information Protection Management System

c) The bidder must have proof of the necessary eligibility, experience, and expertise in providing the service, with the following credentials:

- The bidder must present Client Satisfaction Ratings for at least three contracts with government agencies or private organizations that are similar to this project.

- The bidder shall submit a valid and current Certificate of Distributorship/Dealership/ Resellership of the product being offered, issued by the principal or manufacturer of the product (if the bidder is not the manufacturer). If not issued by the manufacturer, they must also submit a certification/document linking the bidder to the manufacturer.

5. *Delivery and Training*:

- All items should be delivered within 30 days of receipt of the Notice to Proceed.

- Provide training covering essential items for correct use and day-to-day administration.

- Training materials, product guides, and documentation should be available online.

- Must be done during business hours.

- The course outline should be presented.

- Training must begin upon deployment within ten (10) days of solution delivery and must be coordinated with

CMS. The CMS will provide certification for delivery and training completion.

6. Applicable provisions of the Government Procurement Reform Act (RA No. 9184) and its Revised Implementing Rules and Regulations (RIRR) shall form part of the Terms of Reference.

==========

Technical Specifications:

FEATURES	SPECIFICATIONS	COMPLIANCE
NETWORK ADAPTABILITY		
General	The proposed solution must provide a secure software-defined wide area network solution interconnecting the 3 locations of the agency.	
NAT	The proposed solution must support different modes of NAT: 1) SNAT, DNAT, and bidirectional NAT. 2) One-to-one NAT, one-to-many, many to one, many to many NAT.(Modes 1:1, 1:N, N:1, M:N) 3) NAT46, NAT64, NAT66 4) DNS Mapping	
IPSec VPN		
Dynamic Connection	The product proposed must be able to setup site-to-site VPN in the following scenarios: 1) Static IP to Static IP 2) Dynamic IP to Dynamic IP 3) Static IP to Dynamic IP	
IPSec Mode	The product proposed must support IPSec modes: 1) Main mode; 2) Aggressive mode;	
IPSec ID	The product proposed must support local/peer ID type: 1) IPv4_ADDR (IP address) 2) FQDN 3) User_FQDN	
VPN Status Monitoring	Support monitoring the status of each VPN tunnel. The data monitoring includes: 1) Overview of all the active VPN tunnels 2) Inbound/outbound traffic; 3) Latency 4) Packet loss rate;	
Access Control		
Application Control	The proposed solution should support the application control feature and meet the following specifications: 1) Support application control and	

	can identify & control over 9000 applications. 2) Support admin customize their own application types 3) Typical types of applications that can be controlled include games, P2P, shopping and social networking 4) Should be able to control applications via source/destination IP, username and schedule	
URL Filtering	The proposed solution must support URL filtering: 1) provide at least 70 URL categories , include game, gambling, finance, Pornography etc. 2) Support add customized the URL category. 3) Should include built-in on-premise URL signature database, not only rely on cloud or manually create URL database.	
Connection Control	The proposed solution should support features to control concurrent sessions/connections: 1) Be able to control concurrent sessions/connect by source IP, destination IP, or bidirectional. 2) Be able to set the maximum concurrent session/connection number per IP.	
Geolocation Blocking	The proposed solution should be able to control traffic based on Geolocations: 1) Be able to control the source IP by a geolocation level, that means the device has a database that can identify the access(IP) is from which country/region and specify the deny or allow action 2) The geolocation identifications should be able to support the major countries in the world 3) Support the search feature to help find out a specific IP belong to which region/country 4) Support checking the status of IP that being blocked. 5) Support exclusion of specific IP	

	from the control. 6) The Geolocation IP address database should be able to update online/manually.	
SECURITY PROTECTION		
Intrusion Prevention System	The product proposal must support the IPS feature and meet the specifications below: 1) Built-in IPS signature over 13000 entries on-premises. 2) Support customized IPS signature by regular expression, keywords, protocol, port & direction 3) Support admin change the signature default action (Block/Allow/Disable) by per signature or all signature. 4) User can use CVEID, Vulnerability Name, vulnerability ID, threat level to search for the an IPS signature. 5) The IPS module should be 70+ types of brute-force attack, for example, DB2, MongoDB, MSSQL, MySQL, FTP, IMAP, Jboss, Jenkins, Joomla, Kerberos, SMB, SMB2, Telnet, SSH, RDP, etc. 6) IPS can get up-to-date signature data automatically online via cloud threat intelligence or manually upload a signature package via web UI 7) Support detect DNS tunnel, ICMP tunnel, HTTP tunnel, Webshell encrypted communication, reverse shell.	
Botnet/Advance Persistent Threat Control	The proposed solution must support APT and meet the specifications below: 1) Detection of remote control trojan, malicious URL/domain 2) Support customize ICMP, UDP, SYN packet threshold to identify malicious behaviors 3) The product should support at least 1.5 million malware/botnet signature database on-premise	

	4) The device can connect to cloud threat intelligence and do real-time checks for threats that cannot be identified locally. 5) An APT can effectively identify and block the abnormal traffic within well-known protocols such as RDP, SSL, IMAP, SMTP, POP3, FTP, DNS, HTTP, WEB	
Anti-Virus	The proposed solution must support the anti-virus feature: 1) Support stream based anti-virus with AI-Based anti-virus engine 2) Support protocols HTTP, HTTPS, FTP, SMTP, IMAP, POP3, SMB etc. 3) Support compress file detection, and compressed files with up to 16 layers. 4) Supports scanning files up to 20MB 5) Support detection of virus in mainstream file types, including text, image, music, movie, compressed file, executable file, document, script, etc. 5) Support cloud-based analysis with the file cannot be identified locally 6) Support whitelist by MD5 or URL path.	
Anti-DoS/DDoS	The proposed solution must support anti-DOS/DDOS features, with the following features: 1) Support ARP flood, SYN flood, UDP flood, DNS flood, ICMPflood protection. 2) Support IP/port scan protection. 3) Support detection and prevent a TearDrop attack, LAND attack, WinNuke attack, Smurf attack, Ping of death, IP fragment. 4) Support ARP Spoofing prevention 5) Bad IP option, Bad TCP option prevention	

Web Application Firewall	The proposed solution must support the WAF feature by itself, without additional devices. The WAF protection should meet at least the following specifications: 1) Support protect Web applications running on standard port(80) and other ports. 2) Must be able to support the attack types, such as, XSS, SQL,CRSF, CC attack, OS Command Injection, Webshell, scanner blocker, path transversal, etc. 3) Support WAF-related signature on-premise no less than 4500. And support customizing signatures. 4) Support HTTPS site protection with decryption enabled. 5) Support weak password detection for FTP, Web. Support detects web login with plaintext. Support web brute-force attack detection. 6) Support inspection of "X-Forward-For" header and block the illegal access. 7) Support HTTP request Anomaly detection, SQL injection in HTTP header, POST entity overflow, HTTP header overfloW, etc. 8) Support dedicated PHPH and JAVA deserialization prevention option, not only via IPS signatures. 9) Support Cookie-based attacks by inspecting the cookie attribute to detect the hidden threats. 10) Support built-in Web vulnerability analysis module. Analyzing the web vulnerability without causing extra load (like scanning, spidering) to the webserver. Can generate exportable web vulnerability report.	
Asset Management	The proposed solution can provide automatic asset awareness based	

	on the assets' online/offline status, open port, and access traffic	
Account Protection	The proposed solution must support a dedicated account protection module to identify the abnormal usage of user accounts. 1) Support detection of weak passwords, brute-force attacks, abnormal/suspicious logins, etc. 2) Provide a dedicated dashboard to show & respond to all the account abnormal usage events that have happened recently.	
Ransomware Protection	The proposed solution must support a dedicated ransomware protection module, which can: 1) Automatically scan and detect ransomware-related vulnerabilities, such as high-risk ports, weak passwords, brute-force attacks, etc. 2) Provide a dedicated dashboard to show and respond to all the ransomware-related vulnerabilities 3) Can provide guidance or suggested action to admin, e.g., deploy block action 4) It can help create a ransomware protection security policy automatically.	
Endpoint App Control/Application Containment	The proposed solution provides a correlation with the existing endpoint protection to do endpoint application control, 1) Deploy policy to control proxy applications or other unwanted applications 2) Provide a dashboard to monitor the running & controlled application status	
CORRELATIONS		
Correlation across Endpoint Protection	The proposed solution must be able to correlate with the existing Endpoint protection product. It must be able to launch correlation forensic requests to the existing endpoint solution. When suspicious network traffic is	

	detected, the endpoint protection client will report to the proposed solution about the real process/file/applications that generate the suspicious traffic. Security admin can do operations through the proposed solution to quarantine file/start quick or full scan.	
SECURITY ASSESSMENT		
Passive Vulnerability Scan	The proposed solution must provide a real-time vulnerability analysis or passive vulnerability scan: 1) Detection vulnerabilities based on traffic passthrough, without any active scanning activities to the servers, minimize the extra work load and other impact 2) The vulnerabilities that can be detected include web application vulnerability, weak passwords, improper configuration on web servers, etc. 3) Support generating HTML format reports.	
VISIBILITY, LOG & REPORTING		
Business system security analysis	Support a dedicated dashboard to summarize business system(server) relate security risks, the information provide via dashboard includes: 1) Business system severity level, attack events, vulnerabilities. 2) Stages of Attack to let IT admin understand the security impact 3) One-click to block attackers IP.	
User security analysis	Support a dedicated dashboard to summarize user relate security risks, the information provide via dashboard includes: 1) User severity level, attack types, attack events; 2) Stages of Attack to let IT admin understand the security impact	
Logs	The proposed solution must support built-in log center that can keeps 4 types of logs:	

	1) Access Log (Application control log, user authentication log, SSL VPN log) 2) Security Log (IPS, WAF, Botnet, Email protection, Anti DoS, Web Access) 3) System log 4) Support export log to Excel file.	
Reporting	The proposed solution must support built-in reporting features, which include: 1) Generate comprehensive Security report in PDF format 2) Support security report subscription by email, in daily, weekly, monthly based.	
MANAGEMENT		
Alarms	Support email alarm for: 1) Basics: admin login failure, license expiration, process faults, time inconsistency 2) High Availability 3) Resource overload, Log IO overload 4) Security events: email protection, Intrusion Prevention, WAF, anti-Dos/DDOS	
ACL Policy Optimization	The proposed solution must support the ACL policy optimizer, which helps: 1) Identify the redundant policy, expired policy, conflict policy, etc. 2) Be able to track the ACL policy life cycle, help to track every change that has been done to the ACL policies.	
Certifications		
ISO Certificates	To ensure the maturity of solution technology, the principal must have the following certifications:	
	▪ ISO 9001 Quality Management System	
	▪ ISO/IEC 27001 Information Security Management System	
	▪ ISO 27701 Privacy Information Management System	

	▪ ISO/IEC 20000-1 Information Technology Service Management System	
	▪ ISO 29151 Information Security of Personally Identifiable Information Protection Management System	
MAINTENANCE / TECHNICAL SUPPORT		
	▪ For support and services, the bidder must have the following:	
	▪ Unlimited corrective maintenance/ repair services within the warranty period	
	– Twenty-four (24) hours by seven (7) days (Monday to Sunday) technical support and must meet the following response and resolution time: ▪ Critical incidents <30 minutes ▪ Critical threats <60 minutes ▪ Root cause analysis for all support cases filed.	
	• The bidder must provide full documentation for the Activity Plan on installing patches and upgrades, and Root Cause Analysis of incidents encountered.	
	• The bidder must provide on-site support for installing and deploying software patches and version upgrades.	
	• The bidder must provide a procedure for support and problem escalation	
	• The bidder must provide a procedure for support and problem escalation	
	• Submission of Activity/Service Report within 5 calendar days after rendering service	

	– The bidder must conduct system health checks every quarter with the following scope: ▪ System/ Application patches, fixes, security patches, and alerts ▪ System/ Application profile ▪ Resource utilization ▪ Log analysis • Formal reports on the output of conducted health checks within 5 days	

Technical Working Group for ICT Subscriptions

SSS JOEL N. VILLASERAN

DIR IV EDUARDO ALEJANDRO O. SANTOS

SSII OMAR T. GABRIELES

ITO III JAYVIE NEIL MALICK S. MALICDEM

ITO II CEDRIC S. DELA CRUZ

CMT III JESUS NIÑO CHUA

AO IV RAY CHARLIE V. ALEGRE

Approved/Disapproved:

DARLENE MARIE B. BERBERABE
Solicitor General

Certified Funds Available:

MARIA ADELUEZA O. DACANAY
CAO, OIC - FMS