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 TO A MANAGED SD-WAN AND SECURITY SERVICE EDGE SOLUTION FOR HYBRID AND REMOTE ACCESS

Background:

The Office of the Solicitor General (OSG) operates across multiple locations and relies on continuous, secure, and high-performance connectivity to support mission-critical legal systems, internal collaboration, and cloud-based services. In addition to on-site and branch office operations, OSG now supports work-from-home (WFH) and remote work arrangements, which require secure and reliable access to applications and data beyond the traditional office perimeter. As application usage becomes increasingly distributed across data centers, branch offices, public cloud environments, and remote user endpoints, traditional WAN architectures are no longer sufficient to address evolving requirements for visibility, security, scalability, and operational efficiency.

To respond to these challenges, OSG seeks to adopt a managed Software-Defined Wide Area Network (SD-WAN) solution integrated with Secure Service Edge (SSE) capabilities. The solution must provide an integrated application, network, and user intelligence within a single platform, enabling centralized management, monitoring, and consistent policy enforcement for branch offices, cloud resources, and WFH users. This integrated approach will allow OSG to maintain complete visibility into traffic flows, user experience, and application performance, regardless of user location or access method.

The adoption of a unified and managed SD-WAN and SSE solution will enable OSG to modernize its connectivity and security architecture, reduce operational complexity, and strengthen its cybersecurity posture. This initiative supports the government's digital transformation objectives by establishing a resilient, scalable, and secure access framework that effectively supports both on-site operations and flexible remote work arrangements.

Objective:

The primary objective of this project is to procure a Managed SD-WAN and Secure Service Edge (SSE) subscription that delivers secure, optimized, and highly available connectivity for OSG branch offices, data center resources, public cloud workloads, and WFH and remote users, through a single, integrated platform.

Specifically, the solution shall:

- Deliver integrated application, network, and user intelligence, providing end-to-end visibility across WAN links, branch offices, private data centers, public cloud environments, and remote/WFH endpoints.
- Provide centralized management and monitoring, including real-time analytics, historical reporting, and unified dashboards for performance, security, and user experience.
- Enable automation at the WAN edge and on private and public cloud instances, including dynamic traffic steering, automated failover, and policy-based optimization to maintain service continuity.
- Ensure secure access for both on-site and WFH users through consistent identity-based and context-aware policy enforcement, aligned with zero-trust security principles.
- Support reliable access to business-critical applications without interruption, while simplifying operations through a fully managed service covering deployment, monitoring, maintenance, reporting, and continuous optimization.

The ultimate objective is to establish a scalable, resilient, and intelligent wide-area networking and access platform that enhances user experience, strengthens security, supports hybrid and remote work models, and enables the Office of the Solicitor General to efficiently deliver legal services.

Terms:

1. *Scope.* – Supply and delivery of Subscription to a Managed SD WAN and Secure Service Edge Solution for Hybrid and Remote Access.

2. *ABC.* - The Approved Budget for the Contract (ABC) is **Five Million Pesos (₱5,000,000.00) for twelve (12) months**, inclusive of all government taxes, charges, and other standard fees.

ICT SUBSCRIPTION			
ITEM	**QTY**	**UNIT COST**	**TOTAL**
Subscription to a Managed SD WAN and Secure Service Edge Solution for Hybrid and Remote Access	**1**	5,000,000.00	5,000,000.00
		TOTAL	**₱ 5,000,000.00**

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 fifty percent (50%) of the ABC.

For this purpose, a similar contract shall refer to the procurement contract for any ICT security solution, SDWAN, or firewall.

b) To ensure the maturity of the solution being offered, it must have the following certifications:

- ISO 9001 Quality Management System
- SOC 2 Type 2 Compliance
- ISO 22301 Certification
- Common Criteria EAL4+
- FIPS 140-2 Compliance
- ISO/IEC 27001 Information Security Management System
- ISO/IEC 20000-1 Information Technology Service 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 Certification of Satisfactory Performance for at least three (3) 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 New Government Procurement Act (RA No. 12009) and its Implementing Rules and Regulations (IRR) shall form part of the Terms of Reference.

==========

Technical Specifications:

FEATURES	SPECIFICATIONS	COMPLIANCE
UNIFIED SASE PLATFORM		
	▪ There should be a single unified platform & provide seamless integration of SDWAN+ SSE as a complete SASE solution.	
	▪ The solution should provide a single policy language for users regardless of their connection environment.	
	▪ SASE Cloud gateways should utilize SDWAN to have a view of user traffic for optimally using paths to route traffic.	
	▪ SSE cloud edge device connection type/capabilities - Is it providing SDWAN capabilities or just an IPSec concentrator.	
	▪ The proposed solution must natively integrate enterprise-grade networking and security services, rather than service chaining, cascading, or virtual interconnect between SASE services.	
	▪ The proposed Solution should be ranked in Gartner's Magic Quadrant for SD-WAN, SSE, and Single-Vendor SASE.	
	Common Platform Features	
	▪ The proposed solution should support multitenancy to segment between different networks.	
	▪ The proposed solution must be geo-redundant, and each subscribed location should include redundant POPs or gateways for high resiliency.	
	▪ The solution should be designed for the services for both on-site users and roaming users.	
	▪ The agent or client solution should intelligently connect to the best-performing Cloud POP/ Gateway for traffic inspection and forwarding.	
	▪ The solution must have a Philippine local POP SASE GW	

	▪ In OEM-managed deployment, the maintenance/upgrades of hardware/software delivering SASE services will be the responsibility of the OEM vendor. OEM should notify the customer of upgrade/maintenance activity in prior.	
	▪ The proposed solution should have AI/ML capabilities integrated into the platform.	
Traffic Steering & Application Performance		
	▪ The proposed solution should have the ability to provide end-to-end network performance management and fault detection in real-time.	
	▪ The proposed solution must have application acceleration techniques built-in to optimize real-time network and app performance.	
	▪ The proposed solution should be able to apply QoS policies for SaaS and/or private application traffic from remote or branch users.	
	▪ The solution should support SaaS App optimization	
	▪ The SASE solution should be able to classify traffic based on different criteria like IP/FQDN/Application.	
Multi-Region Architecture		
	▪ The solution should have a global footprint with at least 90 points of presence (POPs).	
	▪ The solution should allow accessing resources outside the local region using the SASE Cloud platform with an SDWAN backbone.	
SDWAN		
General Requirement		
	▪ The network should be implemented as a true software-defined network architecture; the SD-WAN network architecture should have physical separation of management, control and data plane functions. Management and control plane should be centralized with capability to be separated for each tenant in such a	

	way that management, control and data traffic are not intermingled. Management, Control and Data plane must be residing on separate devices so that failure of a single device does not affect other functions. All Component of SD WAN should be on premise.	
	▪ The solution components should include Centralized Network Orchestrator, Software Defined Network Controller, edge devices running in the remote branch locations, Hub/gateway device running in central location	
	▪ The tunnel creation should be automatic without any manual configuration on the edges and the controller, for all topologies including Hub & Spoke, Partial Mesh and Full Mesh	
	▪ The WAN path Selection at the branch locations should be based on the near real-time analytics of the WAN Links Capacity & Quality (Packet loss, Latency & Jitter).	
	▪ The architecture should allow for internet breakout at the local branch, centralized location, remote entity (remote location) based on the application and the policy defined in the software-defined network controller.	
	▪ The solution should allow network service insertion & service chaining to expand the agility and utility of the network. The solution should have the ability to do service chaining with external PNFs or hosted VNFs. The VNF capability should be available on any SD-WAN edge devices.	
	▪ The system architecture should be transport agnostic and should support MPLS, ILL, BB, LTE, 4G/5G SIM card, and other transports.	

	▪ The SD-WAN should support SNMP V3, IPFIX, Syslog exporter, etc. for monitoring and reporting purposes.	
	▪ The SD-WAN solution must be able to apply QoS policies to all the traffic seen in the network, including both optimized and non-optimized traffic flows, including TCP, UDP, and other non-TCP traffic types.	
	▪ The SD-WAN solution should include a QoS mechanism that can protect delay-sensitive flows like Voice, Video, and VDI.	
	▪ The solution must support per-user QoS policy to restrict user traffic.	
	▪ The solution must support restricting user traffic based on source IP and user ID.	
	▪ The SD-WAN should support IPv4 & IPv6 dual stack from Day-1	
	▪ The SD-WAN should support 802.1Q and 802.1X	
	▪ The SD-WAN should support the following IPv6 capabilities * IPv6 addressing architecture, IPv6 name resolution, IPv6 statistics, IPv6 neighbor discovery * ICMPv6, IPv6 DHCP *Support for the following IPv6 features: OSPFv3, BGP Routing support for IPv6, IPv6 Dual Stack	
	▪ The software-defined network controller must have REST APIs available for 3rd party integration or integration with custom automation tools	
	▪ SD-WAN solution should support multi-tenancy. This way the ATM, Branch, and 3rd Party Vendor network can utilize the same Physical CPE, WAN Circuit, and SD-WAN central components with total isolation across management, control, and data plane	
	▪ SD-WAN solution should support route manipulation on LAN, WAN and Overlay to achieve various hybrid network integration requirements.	

	▪ SD-WAN solution should support native firewall to secure the Branch with Direct Internet Access for LAN or Guest users.	
	▪ SD-WAN solution should support Site-to-Site IPSec tunnel on LAN/WAN side with any third-party IPSec-capable appliance for hybrid deployments.	
	▪ SD-WAN solution must come with deep Analytical capabilities with support for on-prem deployment for detailed logging and audit purposes.	
	▪ SD-WAN solution should build dynamic IPSEC tunnels using Asymmetric encryption (DH group) and should generate a unique key for each site for better security.	
	▪ SD-WAN solution should have the capability to mitigate the effect of packet drop in underlay up to some extent for specific or all applications using Forward Error Correction and Packet Replication to improve end-user experience	
	▪ SD-WAN solution must support Hub-Spoke, Full-Mesh, Spoke-Hub-Hub-Spoke and Partial Mesh topologies.	
	▪ The solution should not require the administrator to define the BGP AS number, IPSec authentication password, and the system should automatically bring up the overlay tunnels after the zero-touch process is done.	
	▪ The solution should automatically configure the routing and security policies to enable end-to-end communication for LAN networks over SDWAN between all the sites as per the topology chosen. There should be no manual configuration required to achieve this.	
	▪ There has to be minimum two-factor authentication between Controllers and central and branch devices before they establish communication with	

	each other. Out of two factors, one factor has to be PKI (certificate). The communication between the software-defined network controller and the branch device running on the remote entity should be secure and encrypted	
	▪ The OEM should be in the Magic Quadrant of the latest Gartner's report for Software Defined WAN Edge Infrastructure.	
	▪ The solution should allow Branch sites without a common WAN provider to communicate with each other. (Ex. Branch1 has WAN1 connectivity and Branch 100 has WAN2 connectivity only, then they should be able to communicate with each other)	
	▪ The proposed SDWAN solution must have the capability to support Multicast Features like Multicast forwarding, PIM sparse mode, PIM SSM, PIM rendezvous point, IGMPv2/v3	
	▪ The device must support theft protection and unauthorized movement protection. If the SDWAN device is moved a specific distance from its original location, it must trigger an alarm and should become inactive/unusable	
	▪ SD-WAN solution must support on-premises and on-cloud deployment.	
	▪ SD-WAN solution must support hosting a branch on AWS, Azure, GCP and OCI.	
	▪ SD-WAN solution should have intelligence to route Voice traffic based on MOS (mean opinion score) or similar.	
Virtual Private Network		
	▪ The system should allow creation of multiple virtual private networks/segments as a collection of local area networks present at each branch location and DC HUB location.	

	▪ The system should allow creation of an encryption policy that has a unique encryption key attached	
	▪ The system should allow time-based refresh of the encryption key for each virtual private network	
	▪ The system should only allow dynamic tunnels to be created without any static overlays between branch devices and the hub device.	
	▪ The system should be able to retrieve the network information without any peering protocols like BGP, OSPF, or any other routing protocol over WAN.	
	▪ The system must be able to make virtual private network paths dynamically on power-on without using any routing protocols on the WAN side.	
	▪ The system should support the following encapsulation types: A. IPSEC B. GRE C. UDP	
	▪ The system should support the following authentication algorithms for Data Integrity: a. SHA-512 b. SHA-384 c. SHA-256	
	▪ The system should support the following encryption algorithms for Data Security a. AES-256 b. AES-128 c. Any other FIPS-approved encryption	
Network Performance, Traffic Management & Path Steering		
	▪ The system should be able to prioritize inbound and outbound traffic.	
	▪ The system should be able to select the optimum path based on the network parameters like Latency, Jitter, packet loss, and network capacity.	
	▪ The system should be able to identify business-critical applications and	

	should prioritize this traffic over others during congestion.	
	▪ The system should support packet classification, marking, and bandwidth allocation between SD-WAN devices	
	▪ The solution should support adaptive shaping capability that helps to avoid congestion at the Hub locations. Adaptive shaping allows a device (branch or hub) to enforce a dynamic egress shaping rate on any other device that is sending the traffic. On the sender, only the traffic destined to the device with adaptive shaping configured is shaped and doesn't affect other traffic.	
	▪ The system should ensure that the session is not impacted when switching between paths. In case of blackout or brownout scenarios, traffic convergence to the alternate path should be within sub-second (<1 sec failover time)	
	▪ The system should be able to support multiple internet breakout points based on the application (e.g., the system should do a direct internet breakout at the branch location for Microsoft Office 365 traffic while the rest of the internet traffic should be egressed through a centralized security infrastructure in the data center or the cloud).	
	▪ The system should support load balancing on basis of per packet and per session based on application requirements. Some applications like FTP, which are used for bulk file transfer, should be able to utilize per-packet load balancing to avoid choking of a single link during file downloads; similarly, transaction-based applications like SAP should be able to use per-session load balancing to achieve best performance from the same device	

==========

	▪ The SLA management should have a fallback mechanism in place, i.e., in case both the links at a branch location fail to meet SLA, the traffic should not drop.	
	▪ The solution should support a way to manage flapping links, i.e., remove a link from overlay for traffic forwarding if the link is frequently flapping with incremental times; for example, for the first occurrence the link is out of the path for 1min, for the next occurrence 3 mins or so on.	
	▪ The solution should measure the SLA parameters such as Latency, Packet loss, jitter, and MOS. Each device should do independent SLA calculation towards each remote SDWAN device (bi-directional) on all the paths available to carry traffic. For example, SLA measurement must be done from the Hub device to remote branches as well as from remote branches to the Hub device.	
	▪ The proposed SD WAN solution should do automatic/dynamic encrypted tunnel creation (without any manual configuration) between branch devices to enable branch-to-branch communication (Full Mesh).	
	▪ The proposed SD WAN solution should ensure that any change in physical connectivity (change in service provider or IP address) does not require any change in virtual private network configuration in the SD WAN CPEs at the location.	
	▪ The proposed SD WAN solution should ensure that the virtual private network-specific configuration is not attached to the physical or Virtual WAN IP on the branch device.	
	▪ In the SD WAN solution, the tunnel/VRF creation should be automatic & dynamic without any manual configuration on the edges and the controller.	

	▪ The solution must support SaaS Application monitoring to check the liveliness of SaaS applications as well as determine best path selection towards such applications. SaaS Application Monitor must support HTTP, TCP and ICMP probes to assess both latency and packet loss ratio onto all paths towards SaaS applications (both direct and indirect paths). This monitor must be used to make intelligent decisions about the best path to reach such SaaS applications	
	▪ The solution must support TCP optimization for mitigating the effects of link quality degradation like high latency or packet drops	
SECURITY SERVICE EDGE		
Technical Specification		
	▪ The solution should support different Enterprise Authentication systems - LDAP/AD, Azure AD, ADFS, RADIUS, SAML (Okta, OneLogin, etc.)	
	▪ The SSE Solution must support the creation of local users on the SSE Gateways themselves for the authentication of remote users.	
	▪ The SSE solution must be able to create a local account for Admin users based on domains /emails and allow Admin users to create their own passwords.	
	▪ The SSE solution should have a single user agent for all the features (SWG, CASB, ZTNA, FWaaS etc.) and must be < 50 MB in size. The user agent should be tamperproof, and the user should not be able to disable/bypass the SSE Service even with System Admin Rights.	
	▪ The solution should have a single management/admin console for all the features (, SD-WAN, SWG, CASB, ZTNA, FWaaS and CASB, DLP, etc.).	
	▪ The solution should be able to restrict users based on their geolocation	

	▪ The solution should have device posture validation across multiple parameters like Registry Check, Process Check, AD Domain Check, Certificates, etc., to provide a specific URL or Internet Access based on granular policy controls.	
	▪ The solution must be able to enforce the device posture check irrespective of whether the user is accessing Internet applications or private applications.	
	▪ The solution also must be able to detect not only whether a specific software is installed or not, but also whether it is actually running and is configured.	
	▪ There should be a Philippine Local SSE Gateway.	
	▪ The agent should support both IPSEC and SSL as the tunneling protocol while trying to connect to the gateways for inspection	
	▪ The agent should support both Fail-open and Fail-safe configuration and should be tamperproof i.e., not allow the uninstallation of the agent even with admin credentials till the uninstall password is provided	
	▪ The agent should be supported on all major operating systems, including Windows, Linux, Chrome, MacOS, Android, and IOS.	
	▪ The solution should consolidate and support User identity and identity-based access policy enforcement for both traffic coming from on-premise as well as remote users	
	▪ The solution should provide Middle-Mile optimization to efficiently route traffic to customer datacenter/HQ or SaaS locations	
SSL Decryption	▪ The proposed solution must be able to inspect TLS 1.3 SSL inspection from day 1	
	▪ The proposed solution should allow for the selection of the Key Exchange	

	algorithm, TLS version, the minimum key length, authentication, and encryption ciphers.	
	▪ The proposed solution should allow the administrator to create custom URL categories to allow bypass of certain specific applications from SSL decryption.	
Secure Web Gateway and FwaaS	▪ The proposed solution should have the following security features built into it: a) URL filtering b) IP Filtering c) File Filtering d) DNS Security e) Anti- Malware f) Next Gen IPS g) L7 Next Gen Firewall	
	▪ The proposed solution should have at least 80+ URL categories and should allow the creation of custom URL categories.	
	▪ The DNS Security feature of the proposed solution, apart from using its own malicious domains database, should also cross reference it's URL filtering and IP filtering database for more accurate detection of malicious domains	
	▪ The Next Gen IPS Module of the proposed solution should allow inspection of all traffic, inspection of port and protocol, and should allow the creation of custom signatures, and should allow selection of signatures using multiple parameters such as Year of the CVE, Confidence Score, CVSS Score, OS Product etc.	
	▪ The Next Gen IPS Module of the proposed solution should support both signature and anomaly-based detection.	
	▪ The proposed solution should have an L7 NGFW as an integral part of the offering with more than 3000+	

	Application ID signatures and should not limit itself to only 5 Tupples.	
	▪ The proposed solution L7 NGFW attack detection and mitigation capability should be independently verified by a 3rd party lab and should have at least 99% accuracy in both detecting and blocking the attack.	
	▪ The File Filtering module of the proposed solution should be able to support at least 55+ file types, including XML, torrent, Android, MSI, etc., and should support the following protocols: o HTTP o FTP o SMTP o IMAP o POP3 o MAPI It should also support automated lookup to a cloud database of file hashes in the event that the file hash is not cached on the gateway.	
	▪ The File Filtering module of the proposed solution should allow the administrator to define a custom list of file hashes that should be allowed or blocked.	
	▪ The Anti-virus / Anti-Malware module of the proposed solution should support scanning of more than 60+ file types, including .exe, msi, dll, etc., and should support the following protocols: o HTTP o FTP o SMTP o IMAP o POP3 o MAPI	
	▪ The solution is ready for FWaaS for inbound connections through App Reverse Proxy for agentless access	

	▪ The Antivirus/Anti-malware module of the proposed solution should support both signature and heuristic-based detection and should allow the administrator to define the direction in which the file will be scanned, i.e., Download, Upload, Download & Upload	
CASB	▪ The proposed solution should have 3000+ signatures to accurately identify the SaaS applications being accessed by the users .	
	▪ The proposed solution should support more than 70+ applications, allowing the administrator to granularly control the activity on these applications, like "Login", "Post", "Share", "Comment", "Upload", "Download", etc.	
	▪ The proposed solution should have the capability to distinguish between a user's personal instance /corporate instance for O365 and G Suite and should allow the administrator to restrict access to a user's personal instance for O365/G Suite from agency-owned assets.	
Data Loss Prevention (DLP)	▪ The proposed solution should support at least 100+ predefined data patterns, such as driving license, SSN, credit card, etc., to identify any sensitive information/PII in them.	
	▪ The proposed solution should support at least 15+ predefined compliance standards, including: o GDPR o CCPA - California Consumer Protection Act o PCI DSS o HIPAA	
	▪ The proposed solution should allow for the creation of custom data patterns in Regex and should support at least 30+ file types for scanning.	
Zero Trust Network Access (ZTNA)	▪ The ZTNA module of the proposed solution for accessing private applications should not require the	

	installation of any additional components in the form of any additional virtual machines, daemons, H/W appliance where the private applications are hosted	
	▪ The ZTNA module of the proposed solution should perform security inspection on all traffic coming from the remote user's machine to the private applications, irrespective of port and protocol, and should at least perform the following security checks: o SSL decryption o Anti-Virus/Anti- Malware for any file upload/download to and from the private application. o NGIPS	
	▪ The ZTNA module of the proposed solution should be able to hide the actual IP address of the private application server behind dummy IP addresses.	
	▪ The ZTNA module of the proposed solution should allow the administrator to use specific DNS servers (Internal & External) for the resolution of specific domains.	
	▪ The solution should have dashboards providing information about Applications, Users, and the System's Internal Components	
Reporting and Logging	▪ The proposed solution must have in-built data retention of at least 15 days from day 1 without the need to purchase any additional storage from the vendor.	
	▪ The proposed solution should allow for direct streaming of the Internet traffic and private application traffic logs from the cloud gateways to the on-premises SIEM without the need to install any additional VMs or need to purchase any additional services from the vendor.	
	▪ The proposed solution should offer multiple widgets to allow the	

	administrator to view details such as Top 10 Applications used, Top Threats, etc.	
	▪ The proposed solution should allow for the creation of custom reports and custom dashboards and support scheduled report creation.	
	▪ The proposed solution should be able to display the following statistics from the user's machine to the cloud gateways: a) Latency b) Jitter c) Packet Drop and should also be able to display the average time taken by the Gateway to reach a specific SaaS application. This feature should be an integral part of the reporting engine of the solution and should not require the customer to purchase any additional license	
Solution Integration & Platform Capabilities	▪ The Secure Access Client application must support Android, iOS, Linux, MacOS and Windows operating systems.	
	▪ The Secure Access Client application should support both secure IKEv2 IPsec-based VPN (EAP-MSCHAPv2) and SSL-VPN as the tunnelling protocol while connecting to the cloud SSE gateways for inspection.	
	▪ The Secure Access Client application should be able to intelligently identify the nearest and healthiest gateway by assessing factors like proximity to the gateways, Load per gateway (CPU, Memory, etc.), and automatically establish a connection to the best gateway, which offers the lowest latency and packet-loss between the Client and the cloud SSE gateways	
	▪ The SSE solution shall provide an in-built user directory (IAM service) for short-scale deployments with limited users.	

	short-scale deployments with limited users.	
	▪ The SSE solution should support more than one authentication method for a single tenant, for example, LDAP and SAML, or user and device certificate-based profiles with each other, or with LDAP or SAML authentication profiles.	
	▪ The Secure Access Client application should incorporate additional authentication for users through 2FA or multi-factor authentication MFA using time-based one-time password (TOTP) either via email or Authenticator App TOTP (Microsoft Authenticator, Google Duo, etc).	
	▪ The SSE solution must support user and group-based policy enforcement – Per-user or user group-based access control policies.	
	▪ The SSE solution must allow source geo-location-based access control policies. This allows the enterprise to identify users' location and restrict internet or private application access if the user connects from non-permitted regions.	
	▪ The proposed solution must adhere to zero trust principles & continuously monitor the users and devices posture and other contextual trust, while continuously inspecting the user-to-app or app-to-app data traffic as per the defined access policies to prevent unauthorized access or any kind of malicious content.	
	▪ The SSE solution must be able to restrict the number of concurrent logins per user.	
SSE Client/Agent Capabilities	▪ The Secure Access Client appl+A62+B63:B73+B63:B75+B63:B74+ B63:B73	
	▪ The SSE solution must be able to implement zero-trust policies based on the security posture of the user device. An authorized user with a compliant	

	device can be allowed access, while if the device is not complaint then allow only restricted access or entirely block application access based on the configured policy.	
	▪ The SSE solution must be able to detect not only whether a specific software is installed on a user device but also whether it is configured and is in 'running' status.	
	▪ The SSE solution should be able to integrate with MDM like Microsoft Intune to fetch user device compliance status for posture verification.	
	▪ The Secure Access Client application should be tamper-proof and must not allow users to uninstall the application from their device. Only Network Administrators should have control for troubleshooting purposes.	
	▪ The SSE solution allows creation of custom profiles for device posture checks and also controls or defines what information can be collected from the user device by the Client application for checking the device posture.	
	▪ The SSE solution should be able to support bulk installation of the Secure Access Client application on user machines.	
	▪ The Secure Access Client application should support Fail-Open and Fail-Closed configuration to regulate the private application or internet access on user devices when the Client app is disconnected from the SSE gateways	
	▪ The SSE solution should be able to whitelist applications and domains in the Fail-Closed state.	
	▪ The SSE solution should offer the Trusted Network Identification feature to detect when a user connects from within the Enterprise network and accordingly bypass the Client tunnel creation to SSE gateways and use	

	existing on-prem infrastructure for accessing Enterprise resources.	
	▪ The SSE solution must provide Digital Experience Monitoring DEM feature for analyzing the network connectivity and performance metrics of Enterprise applications(private apps) as well as internet/SaaS applications. This allows Enterprise IT or Admin teams to have complete end-to-end visibility of user-to-app or app-to-app metrics and easily track down issues for faster resolution.	
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:

RYAN C. THOMAS
Director IV - FMS