TERMS OF REFERENCE

Supply, Delivery and Implementation of Network Policy Manager

Background:

Every employee now is utilizing an average of 3 devices such as laptops, smartphones, tablets and other bring your own device (BYOD) that are pouring into the OSG workplace. These devices increase vulnerabilities inside the agency - adding to operational burden.

The goal of the organization is to provide anytime, anywhere connectivity by using our wired and wireless resources without sacrificing security as such, the Office of the Solicitor General is developing its capabilities in network access control with a full-spectrum device visibility across our local area network, as well as to control and response to network attacks.

Objective:

The Office of the Solicitor General requires a **NETWORK POLICY MANAGER** to 1) **identify** all other network objects in the LAN; 2) **enforce** accurate policies that provide proper user and device access; 3) **protect** resources via dynamic policy controls and real-time threat remediation that extends to third party systems.

Approved budget for this project is Three Million Pesos (Php 3,000,000.00).

For the Supply, Delivery and Implementation of Network Policy Manager:

1. The bidder must have completed, within the last 3 years from the date of submission and receipt of at least one (1) single contract of similar nature amounting to at least fifty percent (50%) of the ABC; or the prospective bidder should have completed at least two (2) similar contracts and the aggregate contract amounts should be equivalent to at least fifty percent (50%) of the ABC; and the largest of these similar contracts must be equivalent to at least half of the fifty percent (50%) of the ABC as required.
2. 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 bidder is not the manufacturer). If not issued by manufacturer, must also submit certification/document linking bidder to the manufacturer.

3. The bidder shall have at least one (1) personnel that can support the solution being offered with a certification.

Supply Delivery and Implementation of Network Policy Manager Technical Specifications:

ITEM	QTY	UNIT COST	TOTAL
Network Policy Manager VM Appliance for 1000 users including 1 Year Support	1 Lot	3,000,000.00	**3,000,000.00**
SUB TOTAL			**₱ 3,000,000.00**

ITEM	SPECIFICATION
Technical Specs	• Must be a Role-based network access enforcement for multi-vendor wireless, wired and VPN networks. • Must be a Virtual and hardware appliance that can be deployed in a cluster to increase scalability and redundancy. • Must have an Intuitive policy configuration templates and visibility troubleshooting tools. • Must Support multiple authentication/authorization sources (AD, LDAP, SQL dB). • Must have a Self-service device onboarding with built-in certificate authority (CA) for BYOD. • Must include Guest access with extensive customization, branding and sponsor-based approvals. • Must Support NAC and EMM/MDM integration for mobile device assessments. • Must include comprehensive integration with the Aruba 360 Security Exchange Program. • Must include Single sign-on (SSO) support works with Ping, Okta and other identity management tools to improve user experience to SAML 2.0-based applications. • Must include Advanced reporting and granular alerts. • Must include Active and passive device fingerprinting. • Must have Support for popular virtualizations platforms such as VMware vSphere Hypervisor (ESXi), Microsoft Hyper-V, CentOS KVM & Amazon AWS (EC2).

ITEM	SPECIFICATION
	• Must include Self-registration – highly customizable guest portal • Must have Customizable branding – logos, visual imagery and optional advertisements provide an opportunity to extend company messaging, and promote mobile apps and offers • Must have Automated credential delivery – registration process can deliver SMS text, email or printed credentials depending on security requirements • Must include Mobile device awareness – captive portal is automatically sized for smart phones, tablets and laptops • Must be Industry leading scalability – enterprise and high capacity guest modes provide options for any type of organization • Must include Secure guest access – industry's only login and traffic encryption option for public networks • Must include Social logins – functionality that enables retailers and public venues to gather valuable demographics about guests that opt-in to guest Wi-Fi using Facebook, Twitter credentials • Must include Third-party integration – customizable workflows using rest-based API's for delivering streamlined registration and payment system integration for hospitality and healthcare • Must include Hotspot management – built-in support for commercial oriented guest Wi-Fi hotspots with support for credit card billing • Must Identify who and what connects to the network and ensures that only authorized and authenticated users and devices are allowed to connect to network through automated application of wired and wireless policy enforcement • Must Help administrators centrally configure and manage user profile, security posture, guest, authentication, and authorization services in a single web-based GUI console • Must Provide the ability to create detailed policies by pulling attributes from predefined sources • Must Integrate with multiple external identity repositories such as the Microsoft Active Directory, Lightweight Directory Access Protocol (LDAP), RADIUS, RSA one-time password (OTP), certificate authorities for both authentication and authorization, and Open Database Connectivity (ODBC) • Must provide access to device configuration on a need-to-know and need-to-act basis while keeping audit trails for every change in the network. • Must have collect endpoint attribute data with passive network monitoring

ITEM	SPECIFICATION
	• Must perform security posture assessments to endpoints connected to the network • Must provide the ability to create powerful policies that include, but are not limited to, checks for the latest OS patch, antivirus and antispyware packages with current definition file variables (version, date, etc.), anti-malware packages, registry settings (key, value, etc.), patch management. • Must Support automatic remediation of PC clients as well as periodic reassessments alongside leading enterprise patch-management systems to make sure the endpoint is not in violation of company policies • Must Provide hardware inventory for full network visibility • Must Provide robust historical and real-time reporting for all services. Logs all activity and offers real-time dashboard metrics of all users and endpoints connecting to the network (for 12 months retention) • Must Enable users to self-register and securely onboard multiple devices • Must Supports Windows, macOS, iOS, Android, Chromebook and Ubuntu operating systems • Must have Sponsor-based onboarding allows for custom workflows • Must support Active Directory and cloud identity credential authentication • Must Automate the configuration of network settings for wired and wireless endpoints • Must have Unique provisioning and revocation of device specific credentials and certificates • Must Contain built-in certificate authority specifically for BYOD • Must Use profiling to identify device type, manufacturer and model • Must Provide BYOD visibility and centralized policy management capabilities • Must have centrally enforces all aspects of enterprise-grade access security for any industry. Granular policy enforcement is based on a user's role, device type and role, authentication method, EMM/MDM attributes, device health, traffic patterns, location, and time-of-day. • Must include license that allow secure network access, AAA, RADIUS, TACACS+, Guest Services, Policy Engine and

ITEM	SPECIFICATION
	Enforcement that leverages contextual data based on user roles, devices types, app usage and location for 1000 users • Must include licenses that allow BYOD and IT-issued devices to connect safely to network in compliance with security mandates with flexible policies and unique certificates enable full and limited access based on roles, devices type and security thru automated certificate-based provisioning workflow for 1000 users
Appliance	• Available as virtual appliance. Virtual • Appliances are supported on VMware vSphere Hypervisor (ESXi), Microsoft Hyper-V, CentOS KVM & Amazon EC2. • VMware ESXi 6 up to 6.7 • Microsoft Hyper-V 2012/2016 R2 and Windows 2012/2016 R2 Enterprise • KVM on CentOS 7.5 • Amazon AWS (EC2)
Platform	• Deployment templates for any network type, identity store and endpoint • 802.1X, MAC authentication and captive portal support • Support SNMP-based enforcement on wired switches • Advanced reporting, analytics and troubleshooting tools • Interactive policy simulation and monitor mode utilities • Multiple device registration portals – • Admin/operator access security via CAC and TLS certificates
Framework and Protocol support	• RADIUS, RADIUS Dynamic Authorization, TACACS+, web authentication, SAML v2.0 • RadSec • EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS) • PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAPPublic, EAP-PWD) • TTLS (EAP-MSCHAPv2, EAP-GTC, EAP- TLS, EAP-MD5, PAP, CHAP) • EAP-TLS • PAP, CHAP, MSCHAPv1, MSCHAPv2, EAP-MD5 • OAuth2 • WPA3 • Windows machine authentication • SMB v2/v3 • Online Certificate Status Protocol (OCSP) • SNMP generic MIB, SNMP private MIB • Common Event Format (CEF), Log Event Extended Format (LEEF)

ITEM	SPECIFICATION
Supported Identity Stores	• Microsoft Active Directory • RADIUS • Any LDAP compliant directory • MySQL, Microsoft SQL, PostGRES and Oracle 11g ODBC-compliant SQL server • Token servers • Built-in SQL store, static hosts list • Kerberos • Microsoft Azure Active Directory • Google G Suite
RFC Standards	2246, 2248, 2407, 2408, 2409, 2548, 2759, 2865, 2866, 2869, 2882, 3079, 3579, 3580, 3748, 3779, 4017, 4137, 4301, 4302, 4303, 4308, 4346, 4514, 4518, 4809, 4849, 4851, 4945, 5176, 5216, 5246, 5280, 5281, 5282, 5755, 5759, 6614, 6818, 6960, 7030, 7296, 7321, 7468, 7815, 8032, 8247
Internet drafts	Protected EAP Versions 0 and 1, Microsoft CHAP extensions, dynamic provisioning using EAP-FAST, TACACS+, draft-ietfcurdle-pkix-00 EdDSA, Ed25519, Ed448, Curve25519 and Curve448 for X.509, draft-nourse-scep-23 (Simple Certificate Enrollment Protocol)
Profiling Methods	• Active: Nmap, WMI, SSH, SNMP • Passive: MAC OUI, DHCP, TCP, Netflow v5/v10, IPFIX, sFLOW, 'SPAN' Port, HTTP User-Agent, IF-MAP • Integrated & 3rd Party: Onboard, OnGuard, ArubaOS, EMM/MDM, Cisco device sensor
IPv6 Support	• Web and CLI based management • IPv6 addressed authentication & authorization servers • IPv6 accounting proxy • IPv6 addressed endpoint context servers • Syslog, DNS, NTP, IPsec IPv6 targets • IPv6 Virtual IP for high availability • HTTP Proxy • Ingress Event Engine Syslog source
Support	• Must include 1 Year comprehensive services with 24x7 support
IMPLEMENTATION SERVICES	
I. Project Kickoff	• Review SOW • Define project team • Coordinate schedules • Define project plan