TERMS OF REFERENCE

Network Management System

Background:

The Office of the Solicitor General is developing its capabilities in providing a robust **NETWORK MANAGEMENT SYSTEM** to improve visibility and monitoring its networking assets.

As the Office of the Solicitor General's ICT infrastructure and systems continue to expand, there is a greater need to be able to efficiently monitor and maintain its network resources across OSG offices. A Network Management System will allow the Office of the Solicitor General to effortlessly and remotely monitor and manage its various network equipment and peripherals.

Objective:

The Office of the Solicitor General requires a **NETWORK MANAGEMENT SYSTEM** for network monitoring, policy enforcement, inventory & compliance audit, software management, remote access support, User Administration Tools, Reporting Tools, Asset Management, Mobile Application, 2-Factor Authentication, Access to API, Unlimited SMS alerts.

To meet its objective, the Office of the Solicitor General seeks to acquire a comprehensive **NETWORK MANAGEMENT SYSTEM**.

The budget for this project is Two Million Pesos (Php 2,000,000.00).

For the procurement of Network Management System:

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.

Network Management System Technical Specifications:

ITEM	QTY	UNIT COST	TOTAL
Network Management System (350 License including Network Monitoring and RMM)	1 Lot	2,000,000.00	**2,000,000.00**
SUB TOTAL			**₱ 2,000,000.00**

ITEM	SPECIFICATIONS	COMPLY / NOT COMPLY
PERFORMANCE AND NETWORK MONITORING		
General Features	Solution should be able to monitor processes and services	
	Solution should be able to monitor system performance such as CPU, Memory, Disk and Bandwidth Utilization	
	Solution should be able to monitor hardware and software changes	
	Solution should be able to monitor IP devices uptime and downtime	
	Solution should be able to monitor Windows, VMware, Mac and Linux	
	Solution should be able to trigger an alarm, file a ticket, send an email and run a procedure when an alert is detected	
	Solution supports Port status, port map monitoring, and SNMP traps	
	Solution should idcentify device roles automatically; identified based on device characteristics	
	Supports NetFlow, jFlow, sFlow, IPFIX	
	Solution should be able to display monitoring in a dashboard	
	Solution should be able to provide reports of triggered alerts	
Provides user defined realtime monitoring	Alerts	
	Event Log Alerts	
	Monitor sets	
	SNMP sets	
	System check	
	Log monitoring	

	Monitoring of IP Devices	
	Monitors changes in the configuration of IT system and provides alerts if a change has occurred.	
	Provides alerts via tickets, email, dashboard or run a procedure.	
	Alert on specific file changes and protection violations. · Monitor devices online/offline status	
	Monitor system performance (CPU, Disk Space, Memory)	
	Monitor Processes	
	Monitor Services	
	Monitor Hardware and Software Changes	
	Alert message and recipient configuration	
Automated Network Discovery	Automatically discover all network devices	
Dashboard	Offers view of alerts summary per system (device)	
	Ability to group systems together	
	Customize alerts	
OTHER IMPORTANT FEATURES		
AGENT DEPLOYMENT		
Deployment	Deploy Agent Remotely thru Active Directory	
	Deploy Agent via URL Link	
Agent Installer	Can Bind Administrator Credential inside the Agent package	
	Can Automatically group machine base in Agent package	
SUPPORTED DEVICES		
Workstations, Servers Platform supported	Windows 8/8.1/10	
	Windows Server 2008/2008 R2/2012/2012 R2/2016	
	Apple OS X version 10.7.5 through 10.9 or above. Intel only	
	Network Devices – Routers, Switches, Printers and other IP-based devices.	
	Any SNMP anabled device	
AGENT PROCEDURE		
Procedure Creation	Create IT Procedures/Scripts.	
	Automatically distribute procedures to manage machines, groups of machines within a Local Area Network and/or Remote systems.	
	Able to run CMD, PowerShell, Batch File, VB script commands	
Automated Remediation	Automatically run procedures triggered by an alert (via Real-time monitoring of critical applications, services, event logs) offering automated remediation of issues.	
Scheduling	Schedule procedures to run automatically	

Application Deployment	Deploy Microsoft and non-Microsoft applications	
Policy Enforcement/Configuration Management	Deploy and enforce system policies, configuration, e.g. block control panel, block USBs via Machine, groups of Machine within a Local Area Network and Remote systems.	
File Distribution	Automatically get and distribute files to and from systems connected locally and remotely.	
INVENTORY, ASSET DISCOVERY AND AUDIT		
	Offers comprehensive audit of each system – Hardware, Software Inventory.	
Hardware Inventory	Solution should be able to inventory hardware information such as:	
	System Information (Manufacturer, Product Name, System Version, System Serial Number)	
	Chassis (Chassis Manufacturer, Chassis Type, Chassis Version, Chassis Serial Number, Chassis Asset Tag)	
	Network Information (IPv4 Address, IPv6 Address, Subnet	
	Mask, Default Gateway, Connection Gateway, Country, IP	
	Information Provider, MAC Address, DHCP Server, DNS	
	Server)	
	Motherboard (Manufacturer, Product, Version, Serial Number, External Bus Speed)	
	BIOS Information (Vendor, Version, Release Date)	
	CPU/RAM Information (Processor Manufacturer, Processor Family, Processor Version, CPU Max Speed, CPU Current Speed, CPU, Quantity, Speed, RAM, Max Memory Size, Max Memory Slots)	
	On Board Devices	
	Port Connectors	
	Memory Devices per Slot	
	System Slots	
	Printers Installed on the system	
	PCI and Disk Hardware	
	Disk Volumes	
	Disk Partitions	
	Disk Shares	
Software inventory	Solution should be able to inventory software information such as	
	Software Licenses (Publisher, Title, Product Key, License Key, Version)	
	Installed Applications (Application, Description, Version, Manufacturer, Product Name, Directory Path, File Size, Last Modified)	
	Add/Remove (Application Name, Uninstall String)	
	Startup Apps (Application Name, Application Command, User Name)	
	Security Products (Product Type, Product Name, Manufacturer, Version, Active, Up to Date)	
	Solution should be able to inventory system information such as	

System Information	IP information	
	Disk volume information including drive letters	
	Space available, volume labels	
	PCI and drive hardware information including models, and user editable notes for each device	
	CPU and RAM information with specifics on, CPU speeds, models, number, and ram installed,	
	Printer information with Name, Port and Model	
Custom Fields	Can add additional information Manually or Automatically	
PATCH MANAGEMENT		
General Features	System Compatibility. Whether, the application is agent-based or agent-less it should have a less impact on the performance, stability and compatibility with the current operating environment especially if this will be deployed across a large number of assets or machines.	
	Cross-platform support to patch Windows and Mac operating systems.	
	Ease of deployment and maintenance. The easier the patch management solution is to deploy and maintain, the lower the implementation and ongoing maintenance costs to the organization.	
	Solution should be able to support non-Microsoft products for patching and is able to do seamless deployment of patches – similar approach to a Microsoft application.	
	Solution should use peer to peer technology in deploying patches	
	Solution should be able to automatically download Internet Based patches without worrying network congestion, even machines without direct access to Microsoft.	
	Solution should be able to support patching heterogeneous endpoints such as laptops, desktops, servers, and virtual machines.	
	Solution should have the capability to select type of patch to be downloaded (Critical, Security, hotfix, etc.)	
	Solution should have the capability to schedule a workstation/server reboot whenever patch requires a reboot.	
	Solution should be able to completely automate patching process.	
	Solution should be able to revert deployed patch.	
	Solution has the capability to create patch groups	
	Solution should be able to create test groups to test patches on a small number of endpoints before approving them for deployment.	
	Solution should provide alerts / warnings like or not limited to email notification for new patches	
	Solution should be able to monitor direct patch fix of applications on the server.	
	Solution should provide description of the patch	
	Solution should be able to notify users about patch deployment via notification window	

	Audit Trail and Report. The solution should be able to provide a comprehensive logging facility.	
	Reports should be readily available on an on-demand or per need basis that will help the administrator keep track of the status of software fixes and patches on individual systems. Report can also be customized, or tailored fit based on the requirement on-hand. Solution should provide reports not limited to updated and outdated endpoints, successful and unsuccessful patch count, patch status per endpoint or per group/batch etc.	
Manage Machines	Offers Scan machine, Patch status, Schedule scan, Initial and automatic updates, Pre/Post procedure, Machine History	
Manage Updates	Ability to Machine/Patch updates,	
	Provides Rollback	
	Cancel Updates	
Patch Policy	Create/Delete Policies	
	Approval by Policy	
	Knowledge Based Override	
Automatic and recurring patch scans	Secured or ad-hoc, Scans networks for installed and missing security patches, detects vulnerability, determines which patches are needed.	
	By computer, group or user defined collections of computers	
	Automates the tedious process of researching, identifies which patches are installed and date installed, Monitors and maintains patch compliance for entire enterprise	
Centralized Management of Patches	Does not require multiple patch servers	
	Ensures that all systems are protected, even remote users on laptops and workstations	
	Allows implementation across entire network	
	Always know what patches and security holes reside on each user's system	
Patch approval	Approve or deny selected patches	
	Select by user defined computer collections	
Automated patch deployment	Schedule by time, computer, group or user defined collections of computers	
	Simultaneously deploy all required patches across operating systems	
	Single rollout strategy and policy enforcement	
	Maximize uptime	
Interactive patch management	Select to deploy by patch or by computer	
	Select individual computers, groups or user defined collections of computers	
	Ad-hoc simultaneous deployment of selected patches	
	Across operating systems	

	Across locations	
Flexible configuration	Patch file location, Patch file parameters	
	Reboot actions and notifications, By computer, group or user defined collections of computers	
	Saves bandwidth, Security and policy control	
Comprehensive reports	Graphical with drill-down, User defined	
	Scheduled, E-mail notification	
	Export to HTML, Excel or Word	
SOFTWARE MANAGEMENT		
	Solution should be able to run procedures triggered by an alert (via real-time monitoring of critical applications, services, event logs) offering automated remediation of issues	
	Solution should be capable to create customized IT Procedures / Scripts or use pre-configured procedures	
	Solution should be able to support execution of CMD, Powershell, Batch File and VB Script	
	Solution should be able to easily deploy 3rd party applications	
Cross-platform support	Windows	
	MAC	
	Patches for 3rd party software is included, if made available by 3rd-party software package developers	
Profile base policy	Scan and Analysis Override	
	3rd-Party Software	
	Deployment	
	Alerting	
Scan and Analysis	Can Approve, Review and Reject Patch impact (Critical, Critical, Older than 30 days, Recommended, Virus Removal)	
	Schedule (Daily, Weekly, Monthly)	
Override	Can Approve/Reject Specific KB Override	
	Can Approve/Reject Specific MS Override	
	Can Approve/Reject Specific CVE, Product, or Vendor	
3rd-Party Software	Deploy popular 3rd-party software packages for Windows systems	
	Reboot Options	
Deployment	Warn user and wait for x min and then reboot	
	Reboot immediately after update	
	Ask user about reboot and offer to delay	
	Ask permission, if no response in x min reboot	
	Skip reboot	
	Do not reboot after update, send email	

	Schedule : Daily, Weekly, Monthly	
Alerting	New patch is available	
	Deployment fails	
	OS Auto Update changed	
	Create Alarm	
	Create Ticket	
	Email Recipients	
	Run a Procedure	
Management	Dashboard	
	Patch Approval	
	Patch History	
REMOTE ACCESS		
General Features	Solution should be capable of remoting a managed machine	
	Solution should be able to set remote control policies such as Silent take control, ask permission, approve if no one is logged in,	
	require permission, denied if no one is logged in	
	Solution should be able to record a remote session	
	Solution should be able to access the command prompt without disturbing the user	
	Solution should be able to access and modify the registry, services and processes without disturbing the user	
	Solution should be able to get audit information of the remote system without disturbing the user	
	Can do remote using a mobile application	
Capability to access remote systems without disturbing the user	Access to Command Prompt	
	Access to Asset Summary	
	Access to Registry	
	Access File Manager (Download, Rename, Delete, Move, Copy,	
	Upload)	
	Access to Task manager	
	Access to Processes	
	Access to Services	
	Easy administration of users and policies	
	Access computers from anywhere	
	Password protected	
	Access computers from anywhere	
	Private Remote-Control Session for Windows	
	Remote Control Session is Logged	
	Supports Multiple Monitors	
	Supports Keyboard Mapping and Short-cut	
	Secure Communications	
	Provide the end user control and security to enable or disable remote control functions until granted approval	

REPORTS		
REPORTING	Detailed list, table and graphic style reports	
	Hardware and Software Inventory	
	Disk Utilization	
	License Usage and Compliance	
	Network Usage and Statistics	
	Schedule Reports for Automatic Distribution	
	Distribute automatically to selected e-mail recipients	
	Report for all, groups or specific computers	
	Detailed filtering and content selection	
	Add own logo	
	Save reports with selected parameters for reuse	
	Export report data to readable formats	
	Capable of sending Unlimited SMS Notications with no extra cost	
	Capable of email notifications	
ADMINISTRATION		
General Feature	Solution should be able to limit the access to its module and visibility of machines per user	
	Solution should be able to propagate policies automatically without further user intervention once policies are assigned to machines, machine group or organization	
	Solution should be able to provide compliance reports of enforced securities and policies	
Access Management	Multi-tenant Capable	
	Ability to group systems	
	Assign Admin users	
	Ability to assign roles, scope and groups to Admin Users	
	Logs activities of Users using the system	
	Ability to access Admin system remotely	
Centralized Management	Ability to manage, monitor local and remote systems in a single console (without the need for a private connectivity).	
	Ability to deploy policies, monitoring definitions to both local and remote systems using a single console.	
System Security	Compliance to HIPAA and PCI	
	Remote control sessions to end-user machines/servers is encrypted	
	Access to the user and admin web interface is encrypted using industry accepted standards	
	Capable of 2 factor authentication	
Accessibility		
Ease of Access	Accessible thru the program's web based application	
	Accessible thru the program's mobile application	
SUPPORT		

	1 year of updates and support	
Local Support	9 x 5 Phone, Onsite, E-mail and Chat support, One (1) hour response time upon receipt of call	
DELIVERY		
	60 Days upon receipt of NTP	
Training	Knowledge transfer and training for end users (IT) within the 60 day period delivery period.	