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

NETWORK MANAGEMENT SYSTEM

Background:

The Office of the Solicitor General (OSG) recognizes the critical importance of maintaining and enhancing its network management capabilities in the face of a rapidly evolving ICT landscape. As the OSG's ICT infrastructure and operational scope expand, a robust Network Management System (NMS) becomes even more evident. The existing capabilities must be renewed and fortified to enable the OSG to maintain complete visibility and control over its networking assets efficiently.

With the expansion of OSG offices and the increasing complexity of network resources, adopting a Network Management System has become imperative. This system will empower the OSG to monitor and manage various network equipment and peripherals seamlessly and remotely. Doing so will ensure the integrity, performance, and security of the OSG's network infrastructure, allowing the organization to effectively fulfill its legal and administrative responsibilities.

Objective:

The primary objective of the Office of the Solicitor General is to acquire a comprehensive and state-of-the-art Network Management System. This NMS will serve as a pivotal tool for achieving various critical functions and goals, including:

- **Network Monitoring:** The NMS will provide real-time visibility into the OSG's network, enabling proactive monitoring and rapid issue identification, thereby minimizing downtime and disruptions.

- **Policy Enforcement:** The system will enforce network policies consistently across all OSG offices, ensuring compliance with regulatory and security standards.

- **Inventory & Compliance Audit:** It will maintain an up-to-date inventory of network assets and facilitate compliance audits to meet legal and regulatory requirements.

- **Software Management:** The NMS will streamline software deployment, updates, and license management, enhancing operational efficiency and reducing security risks.

- **Remote Access Support:** Remote troubleshooting and support capabilities will improve responsiveness and minimize on-site visits, ultimately reducing operational costs.

- **User Administration Tools:** It will offer user-friendly tools for user provisioning, authentication, and access control, ensuring secure and efficient user management.

- **Reporting Tools:** Robust reporting capabilities will provide insights into network performance, resource utilization, and compliance status, facilitating informed decision-making.

- **Asset Management:** The NMS will enable effective asset tracking and management, optimizing resource allocation and reducing unnecessary expenditures.

- **Mobile Applications:** Mobile access to network management functions will empower OSG staff to monitor and manage network resources on the go.

- **Multi-Factor Authentication:** Ensuring secure access to the NMS will be a priority, and multi-factor authentication will be a fundamental security feature.

- **API access:** Open APIs will allow seamless integration with other systems and tools, enhancing overall ICT infrastructure efficiency.

- **Unlimited SMS Alerts:** The NMS will provide flexible alerting capabilities through SMS, ensuring that critical events are promptly communicated to relevant personnel.

To accomplish these objectives effectively, the OSG recognizes the need to comprehensively renew and upgrade its Network Management System.

TERMS:

1. *Scope.* – Supply and delivery of eight hundred (800) NMS and RMM Licenses

2. *ABC.* - The Approved Budget for the Contract (ABC) is **Six Million and Five Hundred Thousand Pesos (₱6,500,000.00)**, inclusive of all government taxes, charges, and other standard fees.

ICT SUBSCRIPTION			
ITEM	**QTY**	**UNIT COST**	**TOTAL**
Network Management System	**1 Lot**	6,500,000.00	**6,500,000.00**

(800 NMS and RMM Licenses)			
		TOTAL	**₱ 6,500,000.00**

3. *Delivery:*

   a. All items should be delivered within 10 days of receipt of the Notice to Proceed.

4. *Support and Warranty*

ICT SUBSCRIPTION	
Warranty	1 year of updates and support
Local Support	24 X 7 support through phone, chat, and web-remote assistance for regular and critical incidents
SLA	<table><tr><th>SLA Target</th><th>Low</th><th>Medium</th><th>High</th></tr><tr><td>Initial response tiem and ticket creation</td><td>1 working hour</td><td>1 working hour</td><td>1 working hour</td></tr><tr><td>Resolution</td><td>3 working days</td><td>2 working days</td><td>1 working day</td></tr></table>
Availability	The system shall be up and running with availability level of 99.75% or with one (1) hour and forty-nine (49) minutes of service downtime per month except for scheduled downtime due to preventive maintenance.
Rebate	One percent (1%) of the pro-rated ABC for affected month in excess of twenty four (24) hours of non resolution from initial response and ticket creation.

5. *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
All bid prices shall be considered as fixed prices and, therefore, not subject to price escalation during contract implementation.	
The supplier shall be paid in full, subject to deduction of applicable taxes, upon the issuance by the OSG of the corresponding Certificate of Acceptance 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.	

6. *Qualifications of the Supplier*:

a) The bidder must have completed, within the last three (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.

For this purpose, a similar contract shall refer to procurement contract of Network Management System.

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

c) The bidder shall submit three (3) client satisfaction surveys.

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

7. 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:

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 identify 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	
	Solution should be able to provide seamless navigation and provide detailed statistics and status listed in the systems	
Provides user-defined real-	Alerts	

time monitoring.	Event Log Alerts	
	Monitor sets	
	SNMP sets	
	System check	
	Log monitoring	
	Monitoring of IP Devices	
	Monitor changes in the configuration of the 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	
	Clickable Dashboards	

OTHER IMPORTANT FEATURES		
AGENT DEPLOYMENT		
Deployment	Deploy Agent Remotely thru Active Directory	
	Deploy Agent via URL Link and can be distributed thru corporate email notification	

	Deploy Agent using 3rd party application/tool	
	Deploy Agent thru distribution of copies using any medium (like USB drive, CD etc.)	
	Deploy Agent thru sharing of URL link in the corporate authorized conferencing tool	
	Deploy Agent thru sharing of downloaded file in the corporate on-premise repository to avoid using corporate internet bandwidth	
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 and future windows OS release	
	Windows Server 2008/2008 R2/2012/2012 R2/2016 and future Windows Server releases	
	Apple OS X version 10.7.5 through 10.9 or above.	
	Network Devices – Routers, Switches, Printers and other IP-based devices.	
	Any SNMP enabled 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, Java Scripts, ShellScripts commands in 32 and 64 bit analogy	
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, Device Name, OS Version, Model, Product Key, 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	
	BIOS Information (Vendor, Version, Release Date)	
	CPU/RAM Information (Processor Manufacturer, Processor Family, Processor Version, Number of Physical and Logical Cores, CPU Speed, CPU max 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	
	Network Adapters (Name/Brand, Throughput)	
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)	
System Information	Solution should be able to inventory system information such as	
	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, Mac and Linux 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, VB Script, Java Scripts, ShellScripts	
	Solution should be able to easily deploy 3rd party applications	
Cross-platform support	Windows	
	MAC	
	Linux	
	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: at least a minimum of 135 third party applications can be patched	
	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	Clickable 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 AND ALERTING	
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 Notifications with no extra cost	
	Capable of email notifications	
ALERTING	Capable of sending unlimited SMS Notifications with no extra cost via a built-in SMS gateway avoiding delays from integrations	
	Capable of email and mobile app 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, and monitoring definitions to both local and remote systems using a single console.	
System Security	Compliance with HIPAA, PCI, and SOC II	
	Remote control sessions to end-user machines/servers are encrypted.	
	Access to the user and admin web interface is encrypted using industry-accepted standards	
	Has built-in 2-factor authentication and OTP	
Ticketing		
	Have main resolver in the system	
	Single-pane RMM integration	
	Ability to create another ticket resolver	
	Ability to create end-user ticket requestor	
	Can manage the status of the ticket	
	Can set ticket status and status label (new, open, pending, waiting, paused, resolved)	
	Automatic creation of ticket thru email	
	Integration with external ticketing tool through push email	
	Can add contacts by registering email addresses	
	Can send real time updates thru active chat	
	Can set priorities to low, medium, high or none	
	Can copy furnish email addresses for monitoring	
	Can set ticket type whether problem, question, incident, task or none	
	Can delegate ticket assignee	
	Can set severity of the ticket	
	Can search ID number of tickets	
	Capable of automatic resolution of incident	
	Viewable source of the tickets	
	Searchable filters such as ticket ID, organization, requestors, priority, severity, status, date and tags	

	Automatic identification of device requestor	
	Customizable organization structures of requestor	
	Can set tags of the ticket	
	Capable of public and private replies	
	Can see the logs of the ticket	
	Can attach file on the ticket	
	Can add a link on the ticket	
	Can set location or department	
	Can see the deleted tickets	
	Can View tickets assigned to a particular resolver	
	Can view all open tickets	
	Can view unassigned tickets	
	Can view, reject and approve pending tickets sent via email	
	Can create and customize domain for ticketing service	
	Can configure timeframe for "resolved tickets" to "close" status	
	Can configure SLA timers	
	Configurable start of ticket numbers	
	Allow end-users and contacts to attach files on the ticket	
	Allows options for authentication to view attached file in the ticket	
	Configurable technical email response either public or private	
	Can configure systray help request	
	Can set and file event-based triggered tickets	
	Can set and file time based triggered tickets	
	Can create ticket forms	
	Can create multiple resolvers	
	Can generate reports	
	- Open ticket reports	
	- Pending report	
	- Resolution time reports	
	- Resolved tickets report	
	- Technician ticket efficiency report	
	- ticket volume report	
Accessibility		
Ease of Access	Accessible through the program's web-based application	
	Accessible through the program's mobile application and shall be 100% similar functionality-wise to the web-based application	

Technical Working Group for ICT Subscriptions

SSS JOEL N. VILLASERAN

DIR IV EDUARDO ALEJANDRO O. SANTOS

ITO III JAYVIE NEIL MALICK S. MALICDEM

ITO II CEDRIC S. DELA CRUZ

SAO JOY Y. CHUA

CMT III JESUS NIÑO CHUA

AO IV RAY CHARLIE V. ALEGRE

Approved/Disapproved:

MENARDO I. GUEVARRA
Solicitor General

Certified Funds Available:

BERNADETTE M. LIM
Dir IV - FMS