6.2.2.90 GTP of NMS -150 Node

(To be filled up and signed by the Manufacturer & Tenderer, otherwise the offer will not be acceptable)

NMS -150 Node		
S/N	**Name of Items or Related Services**	**Bidder Response**
a)	**Brand**	
b)	**Model**	
c)	**Country of Origin**	
d) Network Performance Monitoring		
1	**Core Monitoring Capabilities**	
1.1	The proposed monitoring solution should be able to monitor: (a) Routers (b) Switches (c) Firewalls (d) Wireless devices (e) Servers (e) Other SNMP-enabled devices	
1.2	Should automatically provide real-time, in-depth network performance statistics after discovery/configuration of devices, including, but not limited to, (a) CPU load (b) Memory utilization (c) Interface utilization (d) Packet loss	
1.3	Should show statistics like interface bandwidth, current traffic in bps, total bytes received/transmitted, etc.	
1.4	Should be able to discover and troubleshoot network paths hop-by-hop for both on-premises and cloud environments for specific TCP connections	
1.5	Should display information including alerting for major routing protocols (BGP, OSPF , RIP, EIGRP) with options to view and search routing tables including VRFs, changes in default routes and flapping routes, router topology, and neighbor statuses	
1.6	Should help with multicast traffic information monitoring and alerting, including topology information, multicast information, route information, multicast errors, etc.	
1.7	Should display device status and interface status by different colors to represent warning and critical status	
1.8	Should monitor hardware health for popular vendors like Cisco*, DELL*, F5*, Juniper*, HP*, etc., and should allow alerting and reporting on hardware health monitoring	
1.9	Should show both real-time details and historical details in form of charts with option to choose the time periods	
1.10	Should be able to discover and monitor both IPv4 and IPv6 devices	
1.11	Should have options to poll using SNMP v1, v2c, v3, and WMI	
1.12	Should have options to configure polling intervals as needed	
1.13	Should have options to specify data retention periods	
1.14	Should have the option to determine device availability using SNMP only	
2	**Network Discovery**	
2.1	The proposed monitoring solution should be able to discover devices in the network with SNMP and ICMP capabilities automatically, on input of: (a) IP address ranges (b) Subnets (c) Individual IP addresses (d) Active Directory*	
2.2	Should not add devices with multiple IP addresses as duplicate nodes but should list all known IP addresses for the node	
2.3	Should allow interface filtering on discovery results to exclude virtual interfaces and access ports and select interfaces based on pattern matching	
2.4	Should have option to automate and schedule discovery process	
2.5	Should be able to automatically imports discovered devices	
2.6	Should prompt in web console on discovery of new devices in network	

2.7	Should use discovered information for creating topology maps	
3	**Graphical User Interface and Customization**	
3.1	The proposed management solution should provide a high-quality graphical user interface with asynchronous view refreshing	
3.2	This web console should be accessible centrally or remotely	
3.3	The web console should allow multiple users to log in at the same time	
3.4	It should have horizontal scaling options available if too many users log in at same time	
3.5	It should allow customization by having options to add/remove sections in web pages as necessary	
3.6	It should provide a unified view of alerts, traps, events, syslog messages in a single page	
3.7	It should give a single, unified view of multicast information, route information, and device information for a device	
3.8	It should quickly highlight devices with issues, based on different properties like response time, CPU load, memory usage, high interface usage, etc.	
3.9	It should allow creation of custom dashboards and restrict views for users based on devices or interfaces, i.e., it should have role-based access	
3.10	It should log user actions and events in the web console for audit purposes and they should be available for alerting and reporting	
3.11	It should allow interactive charting for node, interface, volume charts, etc.	
3.12	It should provide a dynamic dashboard allowing in-depth visibility and correlating disparate historical data points across different part of the infrastructure. The result should be exportable in tabular format.	
3.13	It should allow export of any webpage in console to PDF format	
3.14	It should integrate with Active Directory for user login purposes	
3.15	It should be easy to use and intuitive with drill-down features	
4	**Advanced Reporting**	
4.1	The proposed monitoring solution should provide current and historical out-of-the-box reports for various statistics monitored	
4.2	Should be able to generate/create the report via the web console	
4.3	Should be able to generate statistical reports to be used as reference for future planning or troubleshooting	
4.4	Should allow customization of reports by adding/removing columns, setting filters, specifying timeframes, grouping columns, etc.	
4.5	Should allow advanced customization by providing options to enter custom queries to query the database directly	
4.6	Should have options to save the customized reports permanently and have them accessible in the web console	
4.7	Should allow reports to be sent out on schedule as daily, weekly, and monthly reports	
4.8	Should allow emailing of dashboards created in web console	
4.9	Should be able to configure both charts and tables into a single report	
4.10	Should have options to import/export reports created by other users	
4.11	Should support multiple formats such as PDF, HTML, and CSV	
5	**Advanced Alerting**	
5.1	The proposed monitoring solution should be able to manage and display events/alerts in the web console	
5.2	The alerts and events information should be logged into the database for future reference	

5.3	The alerting mechanism should allow complex conditions and condition groups to be specified for narrowing down the alert condition	
5.4	It should allow custom queries to be entered to create rules against the database	
5.5	It should allow creation of new alerts from scratch and also customizable threshold limits	
5.6	It should allow creation of alerts based on sustained states	
5.7	Should have various actions to be taken, including but not limited to, sending out emails, forwarding SNMP traps, running executables, sending SMS text alerts, playing sound, emailing a webpage, etc.	
5.8	Should have support for variables in alert email message to make the content more self-explanatory	
5.9	Should have the ability to dynamically baseline statistics and automatically set Warning and Critical thresholds	
5.10	Should allow alerts suppression during scheduled maintenance	
5.11	Should allow to Stack Alert that can help reduce alert noise and assist in possible root cause analysis to give a quicker MTTR (mean time to resolution). AlertStack should continually monitors alerts and change events and correlates these using Platform topological information, pulling associated events and alerts together into a single alert cluster.	
6	**Grouping**	
6.1	The proposed monitoring solution should allow grouping of devices by various properties—by department, by location, by name, and by other properties gathered	
6.2	Should also allow adding members to groups on-the-fly by specifying a property which can dynamically change values, like volumes reaching low free space	
6.3	Should be able to define dependencies and relationships between connected devices and interfaces to avoid false-positive email alerts in case of outage	
6.4	Should be able to calculate group availability by averaging the availability of the group members	
7	**Network Maps**	
7.1	The proposed monitoring solution should be able to represent the network pictorially and display performance details of devices in real time	
7.2	Should allow customization of background, icons, etc., and should allow multiple network maps to be nested with drill-down capabilities	
7.3	Should be able to display not just the device status on the map but also status of any other detail obtained through custom MIB polling	
7.4	Should have the capability to display the status of nodes or an aggregated group of nodes over dynamically updated street data	
7.5	Should be able to automatically connect devices by means of topology information gathered during discovery, like Cisco Discovery Protocol or Link Layer Discovery Protocol	
7.6	Should be able to view multicast topology using upstream and downstream device list information	
7.7	Should be able to display devices location on the geographical level and down to street level	
7.8	Should have the ability to show the link utilization as a "weather map"	
8	**Multi-Vendor Support**	
8.1	The proposed monitoring solution should not be vendor-specific	
8.2	The discovered devices should be detected by specific vendor and categorized automatically	

9	**Extensibility**	
9.1	The proposed monitoring solution should allow gathering of custom properties from SNMP-enabled devices by specifying the OID of the properties	
9.2	Should be able to fetch properties from devices without need to import device MIBs into MIB database	
9.3	Should be able to get real-time values, charts, and alerts on these custom properties	
9.4	Should have APIs available to programmatically import/export nodes and do similar functionality	
10	**Application Aware Network Performance Monitoring**	
10.1	Should be able to provide Network Response Time (NRT) and Application Response time (ART) for critical applications	
10.2	Should be able to identify and classify ~1,200 applications out of the box	
10.3	Should have the ability to display aggregate volume metrics per application/node	
10.4	Should have the ability to create custom HTTP applications	
10.5	Should be able to contextually provide QoE data for nodes in Node Details subview	
11	**Additional Components**	
11.1	Should have utilities to view the database, to stop and start application services	
11.2	Should have options to receive, display, and alert on syslog messages and traps from devices	
11.3	Should have wireless reporting option to display wireless, thin, and autonomous access points and their associated clients	
11.4	Should have customized mobile views of console for administrators' immediate viewing	
11.5	Should be able to monitor Cisco switch stack, with the ability to display invidual member switches, power stack, and data stack rings	
11.6	Should be able to report on technologies like Cisco UCS, Energywise feature	
11.7	Should be able to report on virtualized Cisco Nexus 1000V switches, VSAN, Fibre Channel switches like Cisco MDS, Brocade, and McData devices	
11.8	Should be able to monitor cloud-based Meraki wireless infrastructure	
11.9	Should be able to monitor entire VMware and Hyper-V virtual infrastructure, including Virtual Centers, Data Centers, and ESX clusters, and automatically track VM performance	
11.10	Should be able to monitor individual components in F5 BIG-IP load-balancing environment	
11.11	Should be able to monitor individual components in Cisco ASA firewall, including but not limited to: connection count, site-to-site and remote access VPN tunnels, interface identity and utilization, high availability status, and configuration synchronization status.	
11.12	Should be able to monitor Cisco Nexus with VDC awareness, including vPC specific view for configured vPC and peer vPC.	
11.13	Should be able to monitor SDN environment (e.g., Cisco ACI), including, but not limited to: APICs, tenants, application profiles, endpoint groups, and physical entities	

11.14	Should be able to monitor SD-WAN environment (e.g., Meraki , VeloCloud ,Viptella and Prisma SD-WAN (formerly CloudGenix)), including, but not limited to: WLC , cloud orchestrator information ,Warm Spare and Tunnels Status	
12	**Integration**	
12.1	Should be able to integrate with modules serving other monitoring purposes and provide a single-pane-of-glass view	
12.2	Should allow integration with third-party applications at user-interface layer, through message exchanges and also through APIs	
12.3	Should be able to integrate with ServiceNow, with the ability to automatically create incidents and synchronize the acknowledgement of incidents bidirectionally	
12.4	It should support multi-factor authentication, including SAML 2.0 for integration with Active Directory Federation Services (AD FS) or Okta for Single Sign-On (SSO)	
12.5	Should be able to use SHA256/512 support for SNMPv3 polling for Secured polling	
12.6	Should provides Verbs for managing common credentials, to integrate with PAM and Vault solution	
	Should supports the Kerberos protocol for WMI authentication.	
13	**Enteprise Scalability**	
13.1	The proposed monitoring solution should be able to accommodate growth through addition of load-balancing applications	
13.2	Load-balancing engines should handle interruptions in the connection between the engines and the main application	
13.3	Should allow information from multiple instances of application to be consolidated into a single view	
13.4	Should support multiple deployment options: (a) Centralized deployment (b) Distributed deployment (c) Hybrid deployment With a centralized operations console view, alert acknowledgement, and reporting interface	
14	**Platform Security**	
14.1	Should be fully compatible with TLS 1.2, without any dependency on TLS 1.1 or 1.0	
14.2	Should support Microsoft® Device Guard with all binary signed to ensure code integrity	
15	**Deployment**	
15.1	Should be deployable within one hour and shouldn't require consultants for deployment, implementation, configuration, or customization	
15.2	Should support agentless deployment	
15.3	Should support deployment on Amazon® EC2 and Microsoft Azure (optional)	
15.4	Should support centralized upgrade for all remote components (e.g. remote data collectors, web consoles) without additional management operation on the remote servers	
15.5	Should include actionable dashboard to provide self-check functionality for the monitoring platform and display remediation advice for non-compliant items	
16	**Frequency of Updates**	
16.1	New features to be added to product versions frequently, preferably twice every year or more	
16.2	Should notify availability of new versions in the web console	

17	**Product Support**	
17.1	Should provide 24/7 support	
17.2	Active support through forums and community would be a welcome feature	
18	**Product Compliance**	
18.1	Should have option to operate in FIPS mode, which limits and discloses the encryption algorithms used	
18.2	Should have achieved certification under Common Criteria Scheme Evaluation Assurance Level (EAL) 2+	
18.3	Should have achieved certification on the Department of Defense Information Network (DoDIN) Approved Products List (APL)	
e) Server & Application Monitor		
1	**Core Monitoring Capabilities**	
1.1	The proposed monitoring solution should be able to monitor: (a) Application status (b) Application performance statistics (c) Services and processes (d) OS performance (e) Hardware	
1.2	Should automatically provide real-time view of processes running in systems and in-depth application performance statistics after discovery/configuration of applications	
1.3	Should be able to manage the processes, services running in systems and in-depth application performance statistics after discovery/configuration of applications	
1.4	Should automatically provide real-time view of Windows event logs, including the level of the event logs, Event ID, and source	
1.5	Should have expert monitoring methods to point out the status and performance of key parameters (like services, queue length in case of Exchange, SQL queries in case of databases, etc.) of applications based on best practices	
1.6	Should be able to put together important parameters of an application, into a single monitoring template to be uniformly applied to applications on different servers	
1.7	A customization made in one application's monitoring template should be propagated immediately to all other servers with the application	
1.8	Should allow use of custom scripts with various scripting engine options like VBscript, Perl, PowerShell, etc.	
1.9	Should have options for user experience monitoring for various applications and services, like HTTP, FTP, DHCP, DNS, SQL Server, Oracle, JSON, etc., to find issues before users notice them	
1.10	Should be able to report on hardware details (like CPU, memory, fan state, power, etc.) of servers from popular vendors like IBM, HP, Dell, and VMware Hosts	
1.11	Should have options to poll using SNMP, WMI, and other methods	
1.12	Should display application status and status of important services by different colors to represent warning and critical status	
1.13	Should show both real-time details and historical details in form of charts with option to choose the time periods	
1.14	Should have options to configure polling intervals as needed	
1.15	Should be able to get Disk I/O Performance Metrics for Processes and Services Monitored via WMI	
1.16	Should have options to specify data retention periods	

1.17	Should be able to provide User Audit Event Logging including Terminated Processes, Stopped/Started/Restarted Services, Nodes Rebooted Newly Created/Edited/Deleted Credentials & Application Templates Assigned, Removed, Managed, and Unmanaged Applications	
2	**Cloud Monitoring Capability**	
2.1	Discover and monitor EC2 cloud instances and EBS volumes in AWS via API	
2.2	Discover and monitor Azure cloud service via API	
2.3	Automatically discover and monitor new instances	
2.4	Consolidate view for cloud, hybrid, and on-premises systems	
2.5	Monitor application performance and OS metrics on cloud instances	
2.6	Should be able to monitor Docker, Docker Swarm, Kubernetes, and Apache Mesos container deployments, with the ability to automatically discover containers running on the orchestrator	
3	**Application Discovery / Monitoring**	
3.1	The proposed monitoring solution should be able to discover applications in the chosen servers, apply monitoring for them and start report statistics in few minutes	
3.2	Should have option to find processes either through WMI or SNMP, Performance Counter Monitors, WMI Monitors, VMware Performance Counter Monitors, etc.	
3.3	Should be able to discover application dependencies and connections between application servers, with the ability to monitor both incoming and outgoing connection information on a per-process level	
3.4	Should have option to discover JMX monitors for monitoring Java-based applications like JBoss®, Tomcat, WebLogic®, etc.	
3.5	Should be able to discover email and directory servers, databases, network services, operating systems, VMware ESX servers, etc., automatically by means of built-in monitoring templates	
3.6	Should be able to create and set automatic Calculation of Warning and Critical Thresholds From Baseline Data	
3.7	Should provide indepth monitoring of Microsoft SQL out of the box with the following SQL Error Logs, Individual Database Details Views, Status of SQL Agent, Job Results, Index Fragmentation, SQL Server® Connections	
3.8	Should provide indepth monitoring of Microsoft Exchange mailbox role servers including performance of Information store, database, storage, replication, etc. It should also trend the sent and received emails and attachments for every mailbox user.	
3.9	Should provide indepth monitoring of Microsoft Internet Information Service (IIS) including services, processes, individual website connections and response time, individual application pool, and other statistics like cache and connection	
3.10	Should provide indepth monitoriing of Microsoft Office 365® products including Exchange Mailboxes, mail Traffic, security, subscription status, and mobile device statistics	
4	**Graphical User Interface and Customization**	
4.1	The proposed management solution should provide a high-quality graphical user interface	
4.2	This web console should be accessible centrally or remotely	
4.3	The web console should allow multiple users to log in at the same time	
4.4	It should have horizontal scaling options available if too many users log in at same time	

4.5	It should allow customization by having options to add/remove sections in webpages as necessary	
4.6	It should provide a unified view of alerts, traps, events, etc., in a single page	
4.7	It should quickly highlight applications with issues, based on different properties like down applications, applications with problems, parameters with high CPU, memory usage, etc.	
4.8	It should allow creation of custom dashboards and restrict views for users based on applications, i.e., it should have role-based access	
4.9	It should allow interactive charting	
4.10	It should allow export of any webpage in console to PDF format	
4.11	It should integrate with Active Directory for user login purposes	
4.12	It should be easy to use and intuitive with drill-down features	
4.13	It should have integration options to automatically visualize relevant virtual infrastructure objects such as datastores and storage objects such as LUNs	
4.14	Should provide a dynamic dashboard allowing in-depth visibility and correlates disparate historical data points across different part of the infrastructure. The result should be exportable with a tabular format.	
5	**Advanced Reporting**	
5.1	The proposed monitoring solution should provide current and historical out-of-the-box reports for various statistics monitored	
5.2	Should be able to generate/create the report via the web console	
5.3	Should be able to generate statistical reports to be used as reference for future planning or troubleshooting	
5.4	Should allow customization of reports by adding/removing columns, setting filters, specifying timeframes, grouping columns, etc.	
5.5	Should allow advanced customization by providing options to enter custom queries to query the database directly	
5.6	Should have options to save the customized reports permanently and have them accessible in web console	
5.7	Should allow reports to be sent out on schedule as daily, weekly, and monthly reports	
5.8	Should allow emailing of dashboards created in web console	
5.9	should be able to configure both charts and tables into a single report	
5.10	Should have options to import/exports reported created by other users	
5.11	Should support multiple formats such as PDF, HTML, and CSV	
6	**Advanced Alerting**	
6.1	The proposed monitoring solution should be able to manage and display events/alerts in the web console	
6.2	The alerts and events information should be logged into the database for future reference	
6.3	The alerting mechanism should allow complex conditions and condition groups to be specified for narrowing down the alert condition	
6.4	It should allow custom queries to be entered to create rules against the database	
6.5	It should allow creation of new alerts from scratch and also customizable threshold limits	
6.6	It should allow creation of alerts based on sustained states	
6.7	Should have various actions available, including but not limited to, sending out emails, forwarding SNMP traps, running executables, sending SMS text alerts, playing sound, emailing a webpage, etc.	
6.8	Should have support for variables in alert email message to make the content more self-explanatory	

7	**Grouping**	
7.1	The proposed monitoring solution should allow grouping of applications by various properties—by department, by location, by name, and by other properties gathered	
7.2	Should also allow adding members to groups on-the-fly by specifying a property which can dynamically change values, like volumes reaching low free space	
7.3	Should be able to define relationships between servers and applications to avoid false-positive email alerts in case of outage	
8	**Topology Maps**	
8.1	The proposed monitoring solution should be able to represent the applications pictorially and display performance details of applications in real time	
8.2	Should allow customization of background, icons, etc. and should allow multiple maps to be nested with drill-down capabilities	
9	**Multi-vendor Support**	
9.1	The proposed monitoring solution shouldn't be application-specific	
9.2	The discovered applications should be monitored with built-in monitoring templates created based on best practices	
10	**Extensibility**	
10.1	The proposed monitoring solution should allow custom scripts to be included to extend application monitoring capabilities	
10.2	Should be able to get realtime values, charts and also alerts on these custom properties	
10.3	Should have APIs available to programmatically import/export nodes and do similar functionality	
11	**Additional Components**	
11.1	Should have utilities to view the database, to stop and start application services	
11.2	Should have customized mobile views of console for administrators' immediate viewing	
12	**Integration**	
12.1	Should be able to integrate with modules serving other monitoring purposes and provide a single-pane-of-glass view	
12.2	Should integrate with virtualization monitoring software to provide end-to-end application performance view from the application to the VM to the host	
12.3	Should allow integration with third-party applications at user-interface layer, through message exchanges and also through APIs	
12.4	Should be able to integrate with ServiceNow, with the ability to automatically create incidents and synchronize the acknowledgement of incidents bidirectionally	
12.5	It should support multi-factor authentication, including SAML 2.0 for integration with Active Directory Federation Services (AD FS) or Okta® for Single Sign-On (SSO)	
13	**Enteprise Scalability**	
13.1	The proposed monitoring solution should be able to accommodate growth through addition of load-balancing applications	
13.2	Load-balancing engines should handle interruptions in the connection between the engines and the main application	
13.3	Should allow information from multiple instances of application to be consolidated into a single view	
13.4	Should support multiple deployment options: (a) Centralized deployment	

	(b) Distributed deployment (c) Hybrid deployment With a centralized operations console view, alert acknowledgement, and reporting interface	
14	**Platform Security**	
14.1	Should be fully compatible with TLS 1.2, without any dependency on TLS 1.1 or 1.0	
14.2	Should support Microsoft Device Guard with all binary signed to ensure code integrity	
15	**Deployment**	
15.1	Should be deployable within one hour and should not require consultants for deployment, implementation, configuration or customization	
15.2	Should support agentless deployment	
15.3	Should include optional agent for Windows, Linux (x86), Linux (ARM), and AIX	
16	**Frequency of Updates**	
16.1	New features to be added to product versions frequently, preferably twice every year or more	
16.2	Should notify availability of new versions in the web console	
17	**Product Support**	
17.1	Should provide 24/7 support	
17.2	Active support through forums and community would be a welcome feature	
18	**Product Compliance**	
18.1	Should have option to operate in FIPS mode, which limits and discloses the encryption algorithms used	
18.2	Should have achieved certification under Common Criteria Scheme Evaluation Assurance Level (EAL) 2+	
18.3	Should have achieved certification on the Department of Defense Information Network (DoDIN) Approved Products List (APL)	
f) Others Requirements		
i)	**License Requirements:** The license period shall have at least 03 years and will be calculated from the first day of system handover	
j)	**Operating System & Hardware Requirements:** Should mention the required operating system and hardware platform required for the offered products/solutions.	
k)	**Authorization:** The original Manufacturer Authorization letter with the offered product must be submitted along with the bid	
l)	**Warranty:** **Minimum 3 (Three) years warranty** for service & support.	

[The Tenderer should complete all the columns as required]

Signature:
Name & Designation of tenderer

Signature
Name and Designation of Manufacturer

Duly authorised to sign the Tender for and on behalf of the Tenderer