AI/ML enabled capabilities and features development for NGNMS

1	**Problem Statement**	Development of AI/ML enabled capabilities and features in networks and in network management and integration of the same in CDOT next generation NMS.
2	**Technology Area**	TCP/IP, Optical, 4G/5G Networks, FCAPS, EMS, NMS, OSS, Network Services, SMO, RIC, APIs, Software development tools and frameworks
3	**Project Introduction**	C-DOT Network Management System (CNMS) monitors and manages multi vendor multi technology networks from a central location. It is developed based on Customisable Service Management Platform (CSMP) which is indigenously developed based on Tele Management Forum (TMF) Standards. The CSMP framework needs to be augmented with the capabilities of AI/ML so that the functionality can be utilised as per a specific NMS product requirements. The solution should be a set of modules / executables which are applicable to all telecom network domains in general. The solution shall be ideal for a wide range of use cases like Analysis of current and historical trends, traffic/congestion predictions, study of anomalous patterns of the network and self-diagnose and self healing in general. The modules shall be capable of analyzing images, data shared by drones in realtime etc. The solution should include techniques like 'Reinforcement Learning', 'Classification', 'Supervised' and 'Unsupervised' and all other applicable methods. The solution should be customisable as per the future requirements and should serve to any domain of the network like GPON/IP/MPLS/DWDM/Wireless etc. The solution should be pluggable with existing CNMS products. The core objective of these modules shall be to provide Business Intelligence reports in a common object model and shall be utilized in any kind of CNMS products with minimal customisation. The solution shall be extendable to be used in the analytics of latest wireless technologies like 5G/6G also. The solution shall be able to process text/file/ image/audio/video data and present in a concised dashboards and reports. It should be able to accommodate multiple network conditions and device types. In general, the solution shall be based on relevant standards like TMF/TEC/3GPP etc. standards and open APIs.
4	**Description**	**Key Features**: **1. Performance Data Analysis**

		• Solution should support the analysis of current and historical performance data like CPU usage, Memory utilization, Rechability and / or downtime of the network devices to understand and predict the actual network behaviour patterns and identify if there is any observable deviations in general. **2. Fault Data Analysis** • Solution should analyze the ongoing fault/trap data along with already recorded historical fault data and apply rigorous correlation of fault data to identify the root cause of the scenario and the impact that the root cause is going to have in the overall network. **3. Trouble Ticket Analysis** • The AI/ML solution shall analyze the complete history of all relevant data like Alerts, Tickets wrt a given Network Element or wrt a given location etc. It shall predict ensuing problems like Network Non-Reachability or Service Non-Availability or Service Disruption or SLA Breach etc. Tickets that are going to impact more number of customers and/or leading to device failures etc should be identified. **4. Traffic Data Analysis** • Solution should study the current traffic patterns of the network using tools like netflow, sflow, ipFlow etc. Predicitons shall be made about the network congestion, automatic re-routing if feasible or guidelines on re-routing of the traffic where automatic re-routing is not feasible. **5. Anomalous Detection** • The solution shall utilize all the above data analyses along with the network topology, to identify Anomalous behaviour in realtime. A set of comprehensive dashboards and reports shall be developed to display such cases. Alerting procedures shall be developed / integrated with these identifications to the field operators concerned. **6. Automatic Configuration and Re-Configuration** • Based on the AI analysis and the user confirmation of the anomalous behaviour of the network, the solution should offer possible resolutions by automatic configuration and / or re-configuration of the network devices/routes etc.

		7. Time Series data and Predictions ● Solution should provide Time series and trend charts of all applicable Key Performance Indicators (KPIs) with appropriate colour codings. The solution should also be able to predict the device errors/down times. For example, the bandwidth utilization in a given route shall be captured in time series and predict when the route is going to overflow, identify the root cause of this overflow, provide possible solutions and execute the operations automatically or manually. **8. Log data Analysis to project the Security Status of the Network** ● The solution modules shall analyse syslogs to project the following indicators: ● a) Anomaly Detection: Identify abnormal patterns or log sequences that may indicate hardware failures, misconfigurations, or software crashes. ● b) **Early warning systems:** Predict faults before they occur based on leading indicators in logs. ● c) **Degradation detection:** Identify slow or failing links/services by analysing logs indicating increased latency, jitter, or throughput issues. ● d) **Load prediction:** Anticipate congestion or bottlenecks by detecting usage patterns over time. ● e) **Threat detection:** Spot suspicious behaviours such as brute force attempts, port scans, or privilege escalations using pattern recognition. ● f) **Insider threat identification:** Analyse access logs to detect unusual access patterns or misbehaviour by legitimate users. ● g) **Log reduction and Summarize:** Filter out noise and focus on actionable log entries. Provide concise summaries or timelines of incidents using NLP techniques on logs. ● **9. Image Processing**

		• Solution should be able to process the images that are being captured as part of Trouble Tickets and in other means. • The module shall be capable of processing images that are shared by drones in realtime to identify the nature and patterns of the images being captured. The case can be taken up during the execution period depending upon the requirement. **10. Auto diagnose and Self Healing** • Solution should correlate the performance data, fault data, network topology and the anomalous patterns of traffic and other predicted network errors. Solution should offer to rectify these network errors automatically wherever applicable. If auto correction is not feasible, the solution should provide guidelines to be carried out by field operator to correct the error. Reinforcement techniques should be applied to understand the effect of the solution provided and optimize the solution for future purposes. The model collects the data for fault detection, decision making for recovery of the fault, culminating the performance evaluation by considering current network traffic data, performance metrics (KPIs) like packet loss, security breaches, historical incident records and other existing bottlenecks of the network like node failures or network delays etc to identify the anomalous behaviour of the network. The model identifies the abnormal data points and patterns that indicate equipment failure. The model shall identify future system performance degradation and malfunction patterns from Historical data. With the help of algorithms like “Reinforcement Learning” etc., the system shall develop methods for the network to discover optimal responses to different types of faults. The model shall consider “image processing” to augment the data set or knowledge base for self-diagnose and self-repair techniques. The model shall be able to re-adjust the configurations of the node dynamically, add/delete/modify the nodes in the network as per the requirement of the network. The model shall improve the algorithm performance continuously by using the parameters like, network throughput, latency, error rates or MTTR values etc. after implementing a certain network healing technique. **11. Knowledge Management**

		• AI/ML analysis can be explored to find out the possibility of rectification of the fault by integrating with Knowledge Management module, where users might have mentioned the solutions for a given type of problems based on their on-field experience. Displaying the user most suitable rectification mechanism and allowing him to execute the required steps at NE. **12. Intuitive Dashboards and Reports** • Solution should develop various dashboards to present the analyses and provide hierarchical drilldown features. **13. Network Analytics for 5G/6G Networks** • Solution should develop Analytics for 5G/6G networks which shall be used as an input during 5G service orchestration or network slicing etc. The module shall achieve Network Data Analytics Function (NWDAF) as per 3GPP / O-RAN standards (for example: using Open Air interface) in lab setup. The module shall provide clear insights into the network for optimizing the network performance. The module shall be developed in a most generic way so that it can cater to future networks also. **14. Predictive Compliance & Automated Remediation Intelligence** • W.r.t Mobile Device Management solutions, Enterprises face constant challenges in maintaining device compliance across varied operating systems, patch schedules, and policy baselines. Traditional compliance checks are reactive, identifying violations only after exposure or service disruption. A predictive, ML-based mechanism is required to analyze historical patch data, policy deviations, and device health metrics to forecast potential non-compliance. The system should recommend or auto-execute targeted remediations, like patch deployment, certificate renewal, or configuration rollback, to ensure continuous compliance and reduce manual administrative effort. **15. AI-Driven Anomaly Detection & Risk-Based Device Analytics for Mobile Device Management** • In large enterprise environments, thousands of devices continuously generate diverse behavioural, configuration, and network data. Static rule-based alerts cannot adapt to

		evolving usage patterns or detect subtle, multi-dimensional anomalies. There is a need for AI-driven analytics that learn normal device and user behaviour, detect deviations such as unusual data transfers, root attempts, or VPN bypass, and dynamically assign risk scores. Such intelligence enables proactive threat containment and automated zero-trust enforcement across all managed devices.
5	**Roles & Responsibilities of C-DOT**	C-DOT will provide technical development assistance, and financial support to the project partner(s) selected through a process of evaluation and due diligence conducted by a committee of subject experts. Wherever deemed necessary and depending upon the project type (i.e. co-development or fully outsourced), C-DOT may arrange resources, equipment, training, testing infrastructure, mandatory clearances, statutory permissions, and provide gap funding to the partner(s) i realizing the respective target deliverables. Development costs of the module, whether developed from scratch or derived from existing background technology of partner(s), shall be borne by C-DOT. C-DOT shall use the final solution for integration with production grade software. C-DOT reserves the right to modify and enhance the solution and provide it to C-DOT customers or another Partner(s). C-DOT shall engage with Partner(s) on a non-exclusive basis and shall retain its right to develop similar projects/products through other developmental programs.
6	**Roles & Responsibilities of Partner(s)**	The Partner(s) may build the required module afresh or by modifying pre-existing background technologies available with them. As per the project demand or project type, the Partner(s) may utilize the available test and infrastructure facilities offered by C-DOT with no/some financial implication for its usage. Any simulators or 3rd party softwares that are required for system specific testing and demonstration of solution capabilities, will have to be arranged by the partner(s). All commercial proposals shall include necessary cloud infrastructure cost as per requirements, manpower and cost breakup (Capital, Consumables, Travel, DA, Training, Contingency, Overhead, GST etc.). The proposal should include minimum of one year support for enhancements and capacity building for future enhancements in the product. Participation in the project shall be on a non-exclusive basis. All partner(s) shall be required to demonstrate commitment to the

		project by entering into a formal agreement with C-DOT as per the CCRP policy.
7	**Expected Deliverables**	**System Architecture Document & Design**: Overview of the solution's architecture, components, interfaces, and interactions with other network elements. **Functional Requirements Specification**: Detailed specifications of system functionalities, working and tuning **Solution Source code**: Implementation of multiple modules and relevant APIs for seamless integration. Steps to scale the system, along with the entire working source code of the solution. All the above-mentioned features can be delivered in a phased manner. Standalone modules that do not have any dependency shall be implemented first and dependant modules can be taken up subsequently. **Testing Reports**: Results from functional, performance, and security testing. **User Manual and Training Materials:** Guides for further customization, integration and deployment.
8	**Ownership of Background & Foreground IP**	All technologies created during the project shall be owned by the C-DOT. Any agreement required for collective ownership shall be subsequently settled directly with the concerned partners, but the ownership/IPR of the final solution shall rest with C-DOT only with all the deliverables including complete source code etc.
9	**Timeline for Project**	24 Months from date of approval
10	**Eligibility Criteria of Partner(s)**	Desirable Vendor Requirements for ensuring expertise in the Development and Delivery: 1. Proven industry experience in product development in similar products. 2. Must be members and must have contributed to standard bodies like TSDSI / 3GPP etc. In case of consortium, lead member must have contributed to these standard bodies. 3. Having demonstratable patents is desirable 4. Must be partners of ToT and/or Research oriented programs in the similar field 5. If participating as a consortium, members of the consortium must have complimentary skillset with diverse expertise. 6. The vendor must have been associated with or acknowledged by leading companies working in the telecom networking/service/oss/bss domains 7. Preference would be given to premier academic institutions of National importance.