Request for Proposal

For

Request for Proposal

For

Endpoint Detection and Response Solution for GMDC

RFP Number: GMDC/IT/EDR/01/2025-26

Corrigendum – 2.1

Revision in Bid T&C

Gujarat Mineral Development Corporation

GMDC
FUELING THE GROWTH

GMDC
Gujarat Mineral Development Corporation Ltd.
(A Government of Gujarat Enterprise)

ANNEXURE 1: Amended RFP Specification & Terms

1. Amended Minimum Specification

Sr. No	General Requirement	Compliance or not
1	Proposed solution should be a Leader or Strong Performer in the latest Forrester Wave report of Extended Detection and Response Platforms.	
2	Proposed solution should be in Leaders Magic Quadrant in the latest Gartner report for Endpoint Protection Platform.	
3	The proposed solution should identify and protect GMDC assets from known and unknown threats including but not limited to zero-day, malware, ransomware, filebased and file-less attacks always. Further, response action should be available to remediate the threats in real-time.	
4	The proposed solution should provide a unified console to view the entire chain of events linked to the threat across multiple channels like endpoint, server, cloud, network, etc.	
5	OEM should provide Dedicated SaaS Management Instance for GMDC. However, if required The proposed solution should have facility for on-premises server hosted at GMDC DC/DR to bridge the connections between GMDC intranet (endpoints, server and network) and the cloud. No endpoint, server or network device of the GMDC intranet should directly connect to the cloud.	
6	The proposed OEM (EDR & XDR) should have High-Availability for their cloud hosting within India region itself. The proposed OEM (EDR & XDR) cloud should be offered through MeitY empaneled data center. Solution should have Service Availability is 99.9% in each calendar year. also the telemetry data should be residing in Meity Empaneled Cloud only and should not leave India	
7	The proposed solution should be ISO/IEC 27001:2022 and SOC 2 Type II compliant.	
8	Solution should Provide EPP and EDR capabilities in a single agent without requiring multiple software packages to be installed	
9	The Solution should have Endpoint Security and Identity Security managed in the same console without requiring multiple logins.	
10	The Solution should have Location aware network access - Perform host firewalling basis the location of the system	
11	The Solution should have Data Residency in INDIA	
12	The Solution should have technical assistance center in INDIA	
13	The proposed solution should store all the telemetry data collected from the GMDC environment at MeitY compliant Data Centre in India and analytics should happen in India only.	
14	Proposed solution must be compliant with data localization guidelines of India for all their scoped services such as Data Lake, Management console, sandbox, logs and analytic services.	
15	Proposed solution should not ask for a reboot for a minor version, hotfix upgrade, or post-installation of an agent.	
16	The proposed solution must deliver wide range of detection and response capability across multiple layer (e.g. Endpoint, Servers, network etc.) to provide enhance, efficient and effective visibility to identify low and slow attack.	
17	The proposed solution should provide details of tactics, techniques and procedures used by the attacker and provide mapping of threat / alerts to MITRE ATT&CK framework.	
18	The proposed solution should provide detailed information of system and network level activities to rapidly assess the nature and extent of an attack and subsequently initiate response activities in real-time.	

19	The proposed solution should provide a unified console for threat analysis, forensic analysis, threat hunting, investigation and threat response functionality.	
20	The proposed solution should have a single console for policy management of all the EPP, EDR, Exploit Protection, Anti-APT, Host Firewall, Identify Analytics, Device Control etc	
21	Proposed solution must have unified management console for all action, policy, troubleshooting, threat hunting, Integration etc.	
22	The proposed solution should be able to prioritize incidents / alerts by identifying and highlight the alerts / threat that pose greater risk to the GMDC.	
23	The proposed solution should support detection of advanced malware, zero-day attacks and exploits without requiring signatures at endpoint, server, network and cloud.	
24	The provided solution should support static, dynamic, bare metal, network analysis & recursive analysis etc.	
25	The proposed solution should provide remediation suggestion to assist security teams for remediation / containment of the threat identified in GMDC environment	
26	The proposed solution should provide multi-factor authentication for logging in to the console.	
27	The proposed solution should be able to send alerts/notifications/report over email.	
28	The proposed solution should support creation and configuration of role-based access through the GUI console	
29	The proposed solution shall provide feature to generate, schedule, and view reports based on various parameters captured / stored. Out of the box reports should also be available.	
30	The proposed solution should provide minimum 30 day online raw log / telemetry data retention and minimum 180 days retention for alerts and incident related data (including applicable forensic data). Log retention (as mentioned) is applicable to all the components of the proposed solution.	
31	Proposed solution should have identity analytics to detect user/identity based threats such as lateral movement, and it should have supervised and unsupervised learning capabilities.	
32	Proposed solution must have analytical capability but not to be limited to process, user/identity, device, Network, File, Registry, and Security alerts and should notify/alert as and when any anomaly is identified based on profiling, modeling, or benchmarking.	
33	The proposed solution should provide incident management functionality like adding comments on the incident, change status of incidents like Open, Closed and should support assigning of incidents to different team members within GMDC team.	
34	Proposed solution must support Windows 10, and 11, windows Server 2012R2 to 2022 or latest. Supports Linux OS - Alma Linux, Amazon Linux, CentOS, Debian, Oracle Linux, RedHat, Rocky Linux, SUSE, Ubuntu. Also the proposed solution must support Ventura MacOS, Sonoma MacOS, Monterey MacOS, BigSur MacOS, latest and last two major builds, Android and IOS latest and last major release, Kubernetes (containers), and should have VDI support.	
35	The proposed solution should provide functionality to limit the access to specified IP addresses for accessing the console.	
36	The proposed solution should support demonstration Of Impersonation, Risky User Activities, Credential Misuse, Impossible Travel etc.	
37	The proposed solution should detect malicious user activities including but not limited to stolen or misused credentials, credential harvesting, exfiltration, or brute-force attacks by applying AI/ML techniques	
38	Proposed solution should have timeline view and 360-degree identity view with its user risk score.	
39	The proposed solution must be able to detect and respond to cyber-threats on the endpoints and servers with artificial intelligence and machine learning capabilities that may be missed by traditional security solutions.	

40	The proposed solution must provide behavioral based cyber threat detection and prevention capabilities.	
41	It should support advanced querying language with support for wildcards, regular expressions, JSON, data aggregating, field, and value manipulation, merging of data from disparate sources, and visualization of data with ability for an analyst to easily pivot between views. In addition, it should support granular filtering and sorting capabilities.	
42	The Proposed solution must comprise of below minimum functionalities & deliverables: a) Incident data search and investigations: Search historic and live systems for indicators b) Alert triage or suspicious activity validation: Workflow & orchestrated Integration to and from EDR and external file/indicator validation services c) Suspicious activity detection: Automated threat- intelligence- based match and malicious behavior detection d) Threat hunting or data exploration: Link entities investigated across different systems and additional visualizations e) Stopping malicious activity: Centrally Monitor processes, UAC Logs, detect malicious artefacts and help remove files, prevent execution, conduct network isolation, Manual & script based Remediation f) Stopping malicious activity: Centrally Monitor processes, UAC Logs, detect malicious artefacts and help remove files, prevent execution, conduct network isolation, Manual & script based Remediation g) Incident Live Forensics: Root cause Analysis, Forensic Acquisition, Incident Investigation at scale h) Stacking data & finding the unknown threats: Data Streaming, Data Analytics, Custom IOC sweeps, API access	
43	The proposed solution must have no dependency on signature based solution with typical use cases covered as below -IOC Detection (Malware & Methodology TTP's), -Intelligence feed integration, -Custom IOC creation, -Triaging an alert, -Containment/Isolation of a threat/machine, -Tracking compromised user activity , -Command-line visibility, -Investigating lateral movement, -Data staging and exfiltration, -Suspected anti-forensics activity -Investigating suspected rootkits & backdoors -Data Acquisition - Live Forensics -Hunting exercise like Stacking data & finding the unknown threats based on endpoint and server activity anomalies.	
44	The proposed solution should provide real-time anti-exploit capabilities to protect GMDC assets from exploit attacks including but not limited to memory corruption, logic flaw, malicious code injection/execution, application exploits prevention, DLL Hijacking, etc.	
45	The proposed solution should protect against exploits of unpatched OS and third-party application vulnerabilities and prevent execution of all unauthorized /malicious software, scripts, and dynamic-link libraries (DLLs).	
46	The proposed solution must be able to detect attacks & alert using methodology indicators such as understanding attacks loaded into memory to steal passwords, PowerShell commands usage with arguments run by an attacker for stealing credentials, lateral movement, privilege escalation, etc.	

47	The proposed solution should have 350+ Analytics based IOAs out of the box and also should not charge for any additional IOA rules that needs to be created	
48	The solution should have a remote Host Remediation shell access/CLI session feature available from the EDR console.	
49	The proposed solution shall have the capability to do enterprise-wide search and destroy across multiple endpoints with single search.	
50	The proposed solution should be able to detect and respond to exploit processes that are more complex than a simple signature or pattern.	
51	The proposed solution shall provide protection against exploits including MacOS, Windows, Linux (Ubuntu & Centos Flavors) and processes running in Linux Containers	
52	The proposed solution should have strong anti-evasion capabilities to ensure that no cyber-threat / attack in its pre-execution and execution stage goes undetected.	
53	Lightweight software Agent deployed on endpoints to collect and monitor activity.	
54	Complete Protection Platform (Per Workstation) must have EPP and EDR, with AI based NGAV, Firewall Control, Device Control, Remote Shell, EDR Hunting and Investigation with 24x7 OEM Support	
55	EDR with extended detection and response (XDR) capabilities, analyzing data across endpoints, networks	
56	Must integrate with external threat feeds to enhance detection capabilities, helping detect known indicators of compromise (IOCs) i.e Proposed solution should be able to consume threat intelligence from third party in form of CSV or JSON, and should be able to distribute crowdsourced threat intel from cloud-based malware analysis service to firewall, endpoint agents.	
57	Complete Endpoint Security(Per Server): EPP + EDR, with NGAV Firewall Control, Device Control, Remote Shell, EDR Hunting with 24x7 OEM Support	
58	AI-powered cybersecurity platform, which must include provision to ingest security data from endpoints, cloud workloads, and other sources to establish baselines for normal activity and begin scanning for anomalies or security events. artificial intelligence-driven threat hunting and response capabilities specifically designed to enhance automated and semi-automated security operations	
59	Central system to aggregate and analyze data, either on-premises or in the cloud	
60	Web-based or app-based portal for managing and monitoring endpoint data.	
61	Incident investigation to provide detailed forensic data to analyze the attack's origin, affected assets, and scope. Timeline-based investigation views for incident response teams to trace events	
62	Tools to allow security teams to perform proactive investigations across endpoints.	
63	Should be able to ingest logs for network analysis that could detect suspicious traffic patterns across the network.	
64	Both automated response actions such as isolating the endpoint, killing processes, or removing malicious files & Manual response options for security teams to investigate and remediate threats End -to End encryption for data in transit and at rest	
65	Solution should provide Ability to remediate all operating system changes with a single click and perform corrective action in machine speed. Tool should also be able to undo any system level changes related to the attack (Registry edits, configuration changes etc.)	
66	Protect the endpoint against malware, even when the system is not connected to the network. The agent needs to be fully autonomous meaning it does not need not to have any dependency on Management Server or Cloud or ANY resources external from the Agent to detect and respond appropriately to sophisticated threats (Zero Day, File-less, Ram-based, Zero Day exploits, Ransomware, Miners, Lateral movement, APT) in real time as the threats are detected.	

67	Solution should support a full remote shell for all OS (Mac, Windows, Linux,) and not limit or restrict to set of commands i.e. Proposed solution must support Windows 10, and 11, windows Server 2012R2 to 2022 or latest and versions of Linux.	
68	Tool should reverse destructive data event including but not limited to ransomware with one click. The tool should also recover files that were deleted or encrypted as part of an attack and restore files to their pre-attack state	
69	The solution should provide option to network quarantine a device automatically and manually. also provide flexibility to configure the network quarantine to allow required communication during a network quarantine.	
70	The solution should provide Automated Threat response capabilities	
71	The solution should provide Ability for an analyst to add notes/comments to an event.	
72	Proposed solution should provide Recommended and Aggressive scanning capability of vulnerability protection addressing vulnerability issues and protection against suspicious network activities.	
73	Solution should provide outbreak prevention with capability to limit/deny access to shared folders, block vulnerable ports, deny write access to files and folders, deny access to executable compressed files and creating mutual exclusion handling on malware processes/files.	
74	Proposed solution should provide antivirus update pattern indicator to display the percentage of agents using acceptable virus pattern along with capability to use custom tags and filters to exclude users or endpoints from the pattern display indicator.	
75	The proposed solution shall be able to display the malicious activity of high-risk processes in a temporal graph	
76	The proposed solution shall allow the analyst to actively hunt for threats within the infrastructure based on different hashes like MD5, SHA1 and SHA256, IP address, signer certificate, process ID, original filename and filename on disk, whether has a GUI	
77	The proposed solution must be capable to integrate with SIEM Solution up to the level where SOC analyst able to receive and alerts on the incident/events from EDR/XDR console	
78	The proposed solution should provide a context menu to allow the Administrator/Analyst to execute additional actions directly related to the object type shown in the search details, example: when the administrator selects a filename in the details of the search, the console shows the available response actions, example: collect the file for further analysis, or add a new filter to the query.	
79	The proposed solution should integrate up-to-the-minute intelligence reports from internal and external sources to help identify potential threats to your environment but not limited to the following: a. Internal Threat Intel b. corporate security teams c. Government agencies d. Information sharing organization e. Security researchers f. Security vendors	
80	The proposed solution should support automatic sweeping tasks based on curated intelligence and manual sweeping tasks against custom intelligence to search the environment for IoCs.	
81	The proposed solution should allow the Administrator/Analyst to manually add IoCs such as File Hashes SHA-1, IP Addresses, Domains, and URL's as part of the custom intelligence.	
82	The proposed solution should allow the Administrator/Analyst to build custom intelligence by subscribing to 3rd party intelligence feeds using standards such as STIX/TAXII.	
83	The proposed solution shall be able to manage the Suspicious Object List and Exception List to control the specific information for synchronization.	

84	The proposed solution should allow auto-sweeping of IOCs based threat intelligence reports.	
85	The Solution should have Endpoint Security and Identity Security managed in the same console without requiring multiple logins.	
86	The Solution should have Location aware network access - Perform host firewalling basis the location of the system	
87	The proposed solution shall be able to connect to a monitored endpoint and execute remote commands or a custom script file for investigation	
88	The proposed solution shall support secured remote shell connection on target machines for investigation	
89	The proposed solution should offer granular authorization support to accommodate a wide range of business policies and rules if necessary	
90	The solution should provide Option for on-premises software appliance deployment for highly regulated environments using a proxy component which would act as a median between endpoints and cloud.	
91	Out-of-the-box console support for multi-site configuration,	
92	The Solution should have Telemetry Control - Admin has control to choose which telemetry data will be ingested for threat hunting purposes	
93	The proposed solution shall have Web Console/GUI based remote task manager as response capabilities. Live terminal should support features such as below: -File hash Information collection -Termination of the service -Download of binary -Addition of hash value to block list Etc.,	
94	Devices should be installed and placed directly into a specific device group at time of installation.	
95	Cloud based, real-time Active Directory and AD attack surface monitoring and reduction further supplemented with domain controller-based Identity Threat Detection and Response. i.e. the solution should have: · capability to watch/monitor specific user or group. · capability to distinguish between user, group or endpoint and should show total number of user or group members. · identity analytics to detect user/identity-based threats such as lateral movement.	
96	Proposed solution should be able to monitor, detect RPC calls	
97	Proposed solution should be able to identify / submit unknown files by its own to sandbox or any AI, ML based solution without user/administrator intervention	
98	Proposed solution should support forensics collection from same agent without making any change at endpoint system, and forensic collection should be supported from the date of windows installation.	
99	The proposed solution should support SAML-based single sign-on (SSO) using your corporate account credentials.	
100	The proposed solution shall be able to add, edit, and delete a user account.	
101	The proposed solution shall be able to enable or disable an account	
102	The proposed solution should allow segregation of Duties, must be guarantee from standard users and system administrators.	
103	The proposed solution should support APIs to automate common operations and procedures such as: a. Manage user accounts and roles b. Investigate and triage security events c. Perform responses during investigation and advanced threat hunting	
104	The proposed solution must provide restricted access to APIs to push and pull data to archive customer desired integration scenario.	

105	The proposed solution should have API keys to allow third-party applications to access data through authorized accounts.	
106	The proposed solution should have an API integration available to integrate with various SIEM and SOAR tools.	
107	The proposed solution should have the capability to allow integration with 3rd party solutions via API.	
108	The proposed solution should have an API documentation available online to quickly understand the necessary request and response schemas.	
109	The proposed solution should have single console for below features : - NGAV & EDR - Threat Hunting - Forensic - Network Traffic Analytics - Historical Queries - Identity Analytics - Cloud Workloads & Container Security	
110	The proposed solution is capable of Detection & Prevention Capabilities Against Identity Theft Attacks Such Below: · SSO & AD Session Hijacking · Data Exfiltration · Compromised Credentials · Compromised Devices · Privileged User Monitoring · Unconstrained Delegation · Enumeration (User, SMB, NetBIOS, DNS etc.) · The Printer Bug · Protection against Mimi Katz to Extract the TGT · Pass the Ticket · Pass the Token · Pass the Hash · DC Sync to Domain Compromise · Impossible traveler”	
111	The proposed solution shall have GUI based remote task manager as response capabilities. Live terminal should support features such as below: -File hash Information collection -Termination of the service -Download of binary -Addition of hash value to block list -Delete the file -Send the hash to get the verdict (TI integration) -Execute a python script -Execute a PowerShell script	
112	The proposed solution must provide all capabilities (as per technical requirements of the GMDC) for threat detection and response in a single lightweight agent with minimal /no impact on performance of the endpoints and servers as well as minimal bandwidth requirements for communication with the on-premises server at DC/DR.	
113	The proposed solution should be able to monitor and protect endpoints and servers from threats regardless of their location like on-premises, cloud and roaming / remote.	
114	The proposed solution should provide endpoint agent self-protection to ensure no tampering / unauthorized modifications and should have password protection to disable configuration changes / uninstallation in an unauthorized manner.	

115	The proposed solution should have advanced machine learning capabilities and behaviour-based anomaly detection mechanism to detect cyber threats. It should be independent of signatures.	
116	The proposed solution must provide threat hunting and response capability across all the endpoints and servers of the GMDC.	
117	The proposed solution must continuously collect, analyze and correlate data from the endpoints and servers with activities including file interactions, process execution, network traffic, registry change, user login, installed software, commands executed to identify and block malicious activities.	
118	The proposed solution should have feature to quarantine the endpoint and block all network communication (except with central management console) from/to the endpoint directly from the central console and allow investigation activities to be performed on the endpoint remotely. It should also provide option in central console to restore the network connectivity which was previously isolated / quarantined by the proposed solution.	
119	The proposed solution should be able to identify and terminate malware process and threads in memory, repairing the registry, delete any dropped malware files, remove any services created by malware, restore files damaged by malware.	
120	The proposed solution should be able to identify all the endpoints and servers that are infected with the same threat and display the entire threat attack lifecycle in a single view.	
121	The proposed solution should have the capability to detect threats using AI and ML, prioritize incidents and provide immediate remediation of the threat at the endpoints and servers.	
122	Defends endpoints - on or off the corporate network - against malware, Trojans, worms, spyware, ransomware, and adapts to protect against new unknown variants and advanced threats like crypto malware and fileless malware and support CPU usage performance control during scanning - Checks the CPU usage level configured on the Web console and the actual CPU consumption on the computer i.e. High, Medium and low.	
123	Ransomware rollback: Detects ransomware with runtime machine learning and expert rules to block encryption processes in milliseconds. Rollback/restores any files by taking backup of ransom ware encrypted files and restoring the same before detection also detects script emulation, zero-day exploits, targeted and password-protected malware commonly associated with ransomware having a built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency.	
124	Proposed solution provider should have capability of vulnerability Protection to virtually patch vulnerabilities. It should provide recommended Intrusion Prevention rules based on network performance and security priorities.	
125	The proposed solution should support restoration of the endpoints and servers in case the endpoints / servers are infected by ransomware or by any other cyber-threat / attack.	
126	The proposed solution shall provide anti-ransomware capability.	
127	The proposed solution should provide Pre and post compromise attack visibility (Root Cause Analysis). The root cause analysis methodology should have an interactive GUI with easy-to-use options.	
128	The Proposed solution should support backward and forward matching of IOCs and Custom Behavioral Indicators.	
129	The proposed solution should have the capability for sandbox analysis of suspicious and malicious files along with AI/ML based malware and threat detection techniques.	
130	The proposed solution should automatically perform sandbox analysis of suspicious files without manual intervention.	
131	"The proposed solution shall support automatic collection of the following forensic information from windows machine for further investigation purposes -Recent files (LNK files)	

	-Jump lists -OpenSavePidlMRU -ShellBags -WordWheelQuery -Amcache -Application Resource Usage (SRUM) -Background Activity Monitor -CIDSizeMRU -LastVisitedPidlMRU -Prefetch -RecentFileCache -Shimcache -UserAssist -Windows Timeline -ARP cache -DNS cache -Hosts File -Network Connectivity Usage (SRUM) -Network Data Usage (SRUM) -Browser History (User, Redirected or System generated traffic) -Memory collection (Remote memory imaging & Full memory images including kernel memory, not just user-space)"	
132	Proposed solution should provide intelligence reports from internal and external sources to help identify potential threats in your environment and link it to the published articles for external resources with capability to run manual and auto run.	
133	The proposed solution must be capable to support incident response automation (Playbooks and customized response playbooks)	
134	The proposed solution should have the capability to integrate with either or both cloud and on-premise identity access management (IAM) system for user authentication and access control	
135	The proposed solution console should show the list of exceptions providing at least but not limited to: Creation date, the user who creates the exception, object value, and the filter to which the exception is being applied.	
136	The proposed solution console should allow the Administrator/Analyst to enable or disable Detection Models based on the organization requirements.	
137	The proposed solution should assign a score to the alert and should calculate the score based on the severity of the matched detection model and the impact scope of the alert (such as number of users, number of endpoints etc.).	
138	The proposed solution should provide protection and recovery from threats like ransomware, malware, browser exploits, Advanced persistent threats or any new or anticipated threats. Ransomware protection must not be limited to specific ransomware behaviour /variants.	
139	The proposed solution should automate the day-to-day activities of SOC analysts. The alert level automation should support actions such as: Communication - Send email, Syslog forwarding Alert and Incident Management - Assign incident - Set alert severity - Set alert status Endpoint Response - Isolate endpoint - Retrieve File	

	- Run endpoint script - Run malware scan”	
140	The proposed solution should reverse destructive data event including but not limited to ransomware. It should also recover files that were deleted or encrypted as part of an attack and restore files to their pre-attack state.	
141	The proposed solution shall support the collection of critical forensic data (Prefetch, Jumplists, Amcache, ShellBags, Shimcache, Full memory including Kernel) using the same EDR agent without making any changes in the system (Endpoint Machine) configuration.	
142	The proposed solution should provide automatic aggregation functionality of combining multiple related alerts across data sources (network, endpoint, cloud, identity) into a single unified Incident for easier and swift investigations to GMDC (Vendor to provide live artifact on the console of the provided solution)	

2. Amended Minimum Eligibility Criteria

Sr	Condition	Eligible
1	The bidder should have a minimum average annual turnover of at least Rs. 50 Lac in any last three (3) years i.e. FY 21-22FY 2022-23, 2023-24 and 2024-25. Supporting the fact, the bidder should furnish Audited annual reports for FY 21-22, FY 2022-23, 2023-24 and 2024-25.	Certificate(s) from statutory auditor / CA with all relevant details & copy of 3 of audited annual report to ascertain its turnover & net worth
2	Bidder must have a positive Net Worth for any last three (3) financial year of FY 21-22, FY 2022-23, 2023-24 and 2024-25. Supporting the fact, the bidder should furnish Audited annual reports for FY 21-22, FY 2022-23, 2023-24 and 2024-25.	
3	The bidder shall be the OEM or authorized dealers/distributors for EDR / XDR Solution. Bidders participating in the capacity of authorized dealers/distributors shall enclose Manufacturer's Authorization Form (MAF) for selling/distributing the products.	Manufacturer's Authorization Form (MAF) from OEM for participating in Bid
4	The bidder to provide a minimum of three (3) different client work orders, each workorder involving the supply, installation, testing, commissioning, and AMC support of an EDR/XDR solution for more than 500 endpoints. These work orders must pertain to projects executed within the last three (3) years ending bid submission.	Copy of Work Orders & Completion Certificate from client.
5	The Bidder or its directors have not been blacklisted by any Government/Government Organization during the last 5 years from the date of uploading of RFP. If at any time such declaration is found false, the bid will be rejected or if the contract work is already awarded, it will be terminated forthwith without payment of any compensation and the EMD/SD will be forfeited.	Declaration as per Annexure - D

3. There is No change in Other Terms and Condition of the RFP & Corrigendum Published earlier