Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
1	11	Section 1		Ransomware attacks can be particularly damaging to an organization. During a ransomware attack, hackers will hold a company's assets and data hostage until they pay a ransom, which can be as high as several million dollars. A ransomware sim is designed to help organizations assess the potential impact of a successful ransomware attack. These simulations provide valuable information, such as the average time it takes to detect an attack and how long it takes the company to respond. **Query:** How are you planning to take Ransomware Simulator and what approach is expected by the ISA to be followed?		ISA to suggest the approach methodology for the same as a part of the architecture and policy design. Also conduct assessment for Ransomware attacks as per the specifications defined for VAPT
2	13	Section 3 Project Implementation Timelines		What is expected work day in a week? 5, 6 or 7days in a week?		Six days a week (Monday to Saturday)
3	13	Section 3 Project Implemen		1. Can we change Project Implementation timeline of the phases? 2. Is there any time limit/ cap		It is already mentioned in the SoW that bidder has to give the actual timelines for each of the phases defined.

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
		tation Timelines		define in case GMDC is not ready for ISO Certification as per projected 15-week timeline?		the overall Estimated Project timeline is of One Year
4	40	Section 7		How do you define the successful Bidder to become payable for GMDC because of any claim or application in terms of the provisions or non-compliance of provision of the any Acts and the Rules and Regulations, By-laws or the Orders made there under, applicable from time to time, such amounts shall be recoverable by the Bidder and GMDC will not be responsible for any compensation? EY is responsible for delivering services as per the scope, maintaining compliance as per above clause will be GMDC's responsibility		As per T&C of RFP

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
5	41	SECTION 7 - INSTRUCTION TO ISAs		Penalty clause Penalties for delay in implementation: "Failure to complete the Service Delivery: If the ISA fails to complete the Service Delivery within the time (s) specified in the LOI/Order/Instruction GMDC may, without prejudice to its other remedies under the Agreement, levy as Penalties, a sum equivalent to 1% of the algebraic sum of the cost for the services to be delivered in phases, for each week or part thereof of delay, until actual delivery of performance. The maximum aggregate penalty will not exceed 10% of the algebraic sum of the cost for the service to be delivered at that site. If the delay continues beyond 10 weeks, GMDC may terminate the Agreement. However, GMDC may consider extension of time for completion of the assigned job with justification thereof" EY will share standard GTC while singing the contract		No Change of condition will be accepted. Bidder needs to accept all the terms and conditions defined in Bid

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
6	41	SECTION 7 - INSTRUCTION TO ISAs		Project implementation"The ISA shall provide, log analysis and other associated training required to monitor the security infrastructure to GMDC Personnel at no cost to GMDC. The training schedule, content and modalities will be defined jointly by both the parties. If Certification is required ISA should consider the training costs to train 04 GMDC team members for the same.""It is a turnkey project. The ISA shall be fully responsible for implementing the Project in totality and should include the items and their prices, if not included in Schedule of Requirement to complete the project on turnkey basis. Any claim whatsoever in this regard will not be entertained later."EY will share standard GTC while singing the contract		ISA needs to consider the cost of all these activities in the project costing. No Change of condition will be accepted. Bidder needs to accept all the terms and conditions defined in Bid

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
7	42	Section 7		"On completion of the task, another report should be submitted by mentioning action taken by this person/group of people from external agency, with duration. The ISA is sole responsible for the action taken by such agency on their behalf"EY will not be using any sub-contractor, responsibility of EY will be to provide recommendation which needs to be remediated by the client using SI/OEM/External Agencies/IT team; please confirmDoes Sub Contracting or hiring external agency is allowed by ISA? Since its conflicting with "Assignment & sub contracts Assignment by ISA clause" - The ISA shall not assign or sub-contract, in whole or in part, its rights and obligations to perform under the Service Level Agreement to a third party.		Noted
8	42	Section 7		How will the ISA be responsible for providing the licenses to meet any additional requirements without any additional cost to GMDC? Please elaborate		Please find the updated clause in the Corrigendum 1
9	42	Installation of additional hardware		How will the ISA will be obligated to undertake integration, operation and maintenance for all		Please find the updated clause in the Corrigendum 1

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
				additional equipment if required? Please elaborate		
10	42	SECTION 7 - INSTRUCTION TO ISAs		"Software licenses (wherever applicable) The ISA shall be responsible for providing Software (System Software, Application Software, Device Drivers, IOS, etc.) required, if any, to meet any additional requirements during the currency of the Agreement without any additional cost to GMDC. All license software must be in the name of GMDC. The ownership of any customized software involved will be of the GMDC.""Installation of additional hardware (wherever applicable) During the currency of the Agreement, for any additional requirement of equipment including interface equipment, the specifications will be provided by the ISA. GMDC/The Third-Party Agency will verify suitability of the specifications submitted by ISA and recommend to GMDC for acceptance. The ISA will be obligated to undertake integration, operation and maintenance for all additional equipment if required."Termination for convenience: "Either party may		No Change of condition will be accepted. Bidder needs to accept all the terms and conditions defined in Bid

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
				terminate the said Service Level Agreement at any time by giving sixty (60) days prior written notice to the other Party. Upon termination, the GMDC shall pay to Successful ISA all undisputed amounts for all products and services delivered up to the date of termination."EY will share standard GTC while singing the contract		
11	44	Section 8 Security Hardening (Policy review and Assessment)		1. Will there be a support/access provided from the OEM/SI while reviewing security hardening of CCTV, Biometric device, Access points etc.2. Count of Network devices for hardening which are not accessible from HO office (Remotely) which are located at Mines.		The onboarded vendor managing the CCTV, Biometric will give the details required and rest needs to be done by the ISA Please find the updated clause in the Corrigendum 1 in which details of Existing Infrastructure are updated
12	44	Section 8 Security Hardening (Policy review and Assessment)		Will there be an Application design document, flow diagram, and detailed documentation and support available from the respective application team for hardening of ERP Oracle-EBS, Weighbridge API, Attendance App, Customer portal, PF App and Data Mining software?		The available details will be shared with the onboarded ISA.

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
13	44	Section 8 Security Hardening (Policy review and Assessment)		ISA will conduct assessment and share the recommendation, SI/OEM/External agencies supporting technology/GMDC IT to patch/remediate the issues; please clarify Is ISA is only responsible for Patch assessment or will there be technical person from GMDC who is responsible for the activity? Here ISA is assuming that Patches has to be deployed by GMDC team.		Based on the Gap analysis and report given by the ISA necessary configuration changes/patch management etc. will be done by Existing / onboarded GMDC Agency for respective solution in consultation with GMDC and ISA
14	45	Section 8		Incase of testing cases like DoS and DDoS which is not a recommended test cases for VAPT, ISA might now be able to hold optimum performance of the systems, however the RFP has stated to conduct it. Please elaborate		ISA to conduct the VAPT as per Industry Standards. ISA to submit the scenarios to GMDC for approval.
15	45	Section 8		It is mentioned that test should be done using Black Box testing to assess the functional operating, however some applications may have login functionality for which credentials will be required so we recommend grey box		If required GMDC will share the details with the onboarded ISA
16	46	Section 8		URL monitoring is a part of external brand monitoring, is GMDC looking to perform the activity externally?		Yes

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
17	49	Section 8		How is GMDC planning to perform security assessment for BYOD getting connecting to the network? Please elaborate		The BYOD devices could be Laptops, Tablets, Mobile phones being used by the employees for connecting to the GMDC intranet. These devices need to be scanned as per the processes adapted for Desktops or Wi-Fi enabled devices
18	49	Section 8		"ISA should review the details available in the software to check the status of the Desktops or other endpoints that getting connected to the network and post review of the same the ISA should recommend if Vulnerability testing of the same is needed with Justifications for the same. Based on the recommendations and justification GMDC would decide and permit the ISA to conduct the VA for desktops. And for the same ISA should give the plan and parameters etc. that needs to be accessed" What approach should ISA follow to review the details available in the software and to check the status of the Desktops Please elaborate		Please find the updated clause in the revised RFP

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
19	50	Section 8		Is ISA responsible for Vulnerability assessment and Testing of CCTV NVRs/CCTV Servers, Access and Biometric, IP Phones, IP SCADA systems in mines and all IOT devices getting connected to the network? Can you please share the frequency, number of revalidations and locations where these systems are installed? Can we get a remote connectivity through secure channel inorder to perform the assessment?		Yes, it is in the scope of the ISA. Quantities are mentioned in the price bid section.First assessment needs to be done by the ISA and based on that ISA needs to include the inputs in the Gap analysis report. Second assessment of the same will be post architecture upgrades and necessary corrections.ISA to offer unit rates for the quantities mentioned in the price bid section. GMDC may choose to do Sample Survey for similar category devices.
20	52	Section 8		"Vulnerability Assessment and PET if required for indoor wireless solutions at Head Office and RF Links installed in mines" Can you please share the frequency, number of revalidations and locations where these systems are installed? Can we get a remote connectivity through secure channel in order to perform the assessment? What approach should ISA follow for vulnerability Assessment and PET if required for indoor wireless solutions at Head Office and RF Links installed in mines		First assessment needs to be done by the ISA and based on that he needs to include the inputs in the Gap analysis report Second assessment of the same will be post architecture upgrades and necessary corrections.

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
21	56	Section 9 Security Architecture		Does GMDC expect Designing of Zero Trust Architecture, Detail designing, Access control polices for its resources? ISA are Assuming Access Control Solution (i.e. DAM, PIM and PAM solutions and licencing cost will be own by GMDC).		This scope is associated to Advisory and Design services related to Security Architecture, Basic guidelines are defined. ISA to design the complete architecture and assist GMDC in the bid management process where in they will design the specifications, quantities etc and based on the same GDMC will float the bid and post they will assist in appointment of SI, Configuration design & review and Project management. Apart from that Bidder is supposed to do VAPT for the newly procured solution.
22	57	Section 9		IN BCP-DR as per RFP, "Replication of IT assets associated to Critical Business with planning for backing data from Data center site to DR site as per the business requirement" Any operational changes will be GMDC's responsibility, EY can assist in designing and reviewing the same; please confirm		
23	58	Section 10		What is the expectation from ISA in Project Management with regards to "Assist GMDC in the procurement process"? Is it mandate to deploy certified Project Management Personals (PMC) during the procurement and implementation phase?		Post release of the Order the ISA would supervise all the works being executed by onboarded bidder, Configuration design & review, The quality checks, invoicing checks and recommending GMDC to release the payments as per the RFP payments terms, Acceptance testing are all the part of the PMC process. Yes PMC personals should be deployed as per the Certifications definitions given

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
						in the manpower certification of PQ Criteria
24	59	Section 10		How many trainings and topics are expected to deliver by the ISA for GMDC team members?		Topics needs to be designed and defined by the ISA as part of the security training in line with the guidelines defined in the RFP and industry best practices. Please find the updated clause in the Corrigendum 1 for tentative numbers of training sessions. Review the document for details
25	59	Section 10		Will the trainings and certification be delivered at an additional cost? EY will recommend Third party certification and GMDC will have to take care of the cost		All the training cost will be borne by the ISA Certification assistance documentation design support, policy compliance etc. whatever needs to be done should be done the ISA The certification fee to be paid to the audit and issuance agency will be borne by GMDC Please see the revised RFP for more clarity.

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
26	63	Section 9Section 12		As per RFP, we are considering Security solution tools and Licencing cost to be own by GMDC. For security testing EY will bring their own license tools wherever applicable Following statement is applicable for testing. However, GMDC has to purchase tool wherever applicable."if Licensing is to be done it should be done on the name of GMDC and for that GMDC will not pay any extra cost to the ISA"		You have to consider the cost of all tools. For the same GMDC will not pay any extra charges. Please refer the updated RFP where in the above clause is modified
27	63	Section 12		Can EY charge OPE on an above Bid price? can we charge as actual? As per RFP, For Surveys if required the ISA needs to make all boarding lodging arrangement on his own and GMDC will ensure that at site the necessary officer is present to assist the ISA team members. The ISA should consider all these it its costing and if possible give the brief details of the travel days and costs considered in the bid		All the lodging boarding charges for survey, execution needs to be borne by the ISA. GMDC will not pay anything extra. ISA should consider all the above costs based on the details of the locations given

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
28	57	Section 9		IN BCP-DR as per RFP, Replication of IT assets associated to Critical Business with planning for backing data from Data center site to DR site as per the business requirement Query:1. Does GMDC expect to take control of Backup and Restoration operation along with Identification of Business-critical function and Preparation of DR Plan? 2. Do GMDC expect to Design DR Site, solutions along with the tentative cost structure for the same 3. Will ISA's responsibility only limited to identify Business Critical function and design BCP-DR plan and SOP documentation?		All 3 points needs to be covered in the scope of architecture frame work

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
29	22	Section 6		**Experience of Executing similar works associated to VAPT, Gap Analysis, Cybersecurity architecture Design, Cyber Security Policy Framework design, Compliance certification domain expertise and training management for cybersecurity in Government, PSUs and Corporates in India within the last three yearsOne project of similar nature costing not less than 5 Cr value of assignment to be awardedDocument RequiredCopy of Work Orders / Contracts AND Copy of Completion certificate from Client along with the copy of purchase Order.Query:Is it sufficient if the bidder firm's RFP signing authority/ CA provides a self-declaration/Certificate for experience executing similar work orders in the amount mentioned? For Experience of similar projects in past 3 years, can EY provide one CA certificate mentioning the number of projects that are above 5 Cr?**		Yes, CA Certificate can be issued as per the table given in the annexure Section For CA certified document supporting PO and Completion certificate if not given would be acceptable If No CA certification the supporting PO and Completion certification would be required Refer the updated table in the RFP with comments

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
30	23	Section 6		**CERTIFIED MANPOWERDocument RequiredList of all certified professionals with certification details like name of the certificate, expiry date, experience of the certificate holder in various domains and details of project handled needs to be given in the format as defined in the annexure post the completion of the sections Query:Is it sufficient if the bidder firm's RFP signing authority provides a self-declaration of having CERTIFIED MANPOWER mentioned in the RFP Pre-qualification requirements? Is PF number mandatory? due to data privacy queries, can we declare if they have opted for PF or not without mentioning the PF Number?**		Yes, you can declare the same instead of defining the PF no. List of Certified Personals as per the revised format given in the annexure to be submitted by the ISA on the ISA Letter head that will be duly signed and certified by the HR head. Please find the updated clause in the Corrigendum 1

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
31	32	Section 7		**FINANCIAL CAPABILITIES:** "Average Annual Turnover (As mentioned in the PQ section revenue earned from Cybersecurity services will be considered) of the ISA"**Query: Can we submit certificate from Statutory audit / authorities for FY19-20, FY 20-21, FY 21-22?For FY22-23 (This is in process, we will submit once completed)**		Please find the updated clause in the Corrigendum 1
32	48	Section 8		Is GMDC looking for architecture setup and security policy framework associated to the cloud services		Yes
33	54	Section 8		At what maturity level should ISA establish and define a complete policy that will be enforced by the security team that will make GMDC Digital Forensic ready		The decision will be jointly taken with the Onboarded ISA when the execution plan is being finalized
34	44	Section 8	IT Asset Discovery (For existing infrastructure at all locations)	Does the Asset Discovery Tool to be implement during Phase 1 - exists in the GMDC environment? If not, could the asset discovery be done using industry standard vulnerability scanning tools.	The Asset Discovery can be achieved through multiple approaches.	Please find the updated clause in the revised RFP
35	44	Section 8	Vulnerability Assessment and Penetration Testing	We request to provide details regarding the scope of assessment for the VAPT including the number of applications, websites, etc. Further, please specify if source	We would require this information to drive the effort estimate which would be required	Please find the updated clause in the Corrigendum 1

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
				code review also required as part of the VAPT.		
36	40	Section 7	Payment Terms	We request to consider add/ modify the clause to consider initiating an upfront advance payment during the commencement phase of the project.	This would help us with the initial overheads to facilitate the delivery of the project.	No advance payment will be made to the ISA.
37	40	Section 7	Payment Terms	We would request to cap the penalty at 5% of the total value	While we fully understand the importance of adhering to the agreed-upon terms and conditions, we also believe in a fair and proportional approach to penalties.	No Change. As per RFP T&C
38	NA	NA	Overall RFP	We request you to engage a certification body that would assist in managing overall conflict for this engagement.	This would help to ensure that conflict arising between GMDC and bidder's that could adversely impact the bidding process.	No Change. As per RFP T&C

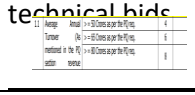
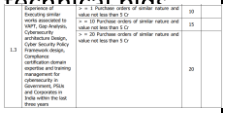
Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
39	Page 14	Section 3 Bidding details	Last date of submission: 15.09.23	Looking to the pre-bid queries and subsequent corrigendum to be issued by GMDC, it may require more time to complete all the risk and legal formalities for bid submission in line with Pre-bid response received from your end. So requesting to extend the bid submission date by atleast 03 weeks from the date of pre bid response. Mail for PWC Team dated 06//09/2023 for extension		Please find the updated clause in the Corrigendum 1
40	Page 13	Section 3 Bidding details	Project Implementation Time line 365 days; It may further be extended on agreement	It is noticed that, the scope is for 67 weeks. Need clarity on Project duration.		Please find the updated clause in the Corrigendum 1
41	Page 18-19	Section 4 - DETAILS OF EXISTING LOCATIONS, USERS AND ITINFRASTRUCTURE	The details of the infrastructure, applications and websites that needs to be assessed are mentioned in the below table:	It is understood that the asset detail as mentioned on page no19. are under scope of work of ISA. If there is more asset/components to be covered under scope of work, May we request to provide the entire asset detail including Infrastructure, devices, Web site, application, end points, IOT devices etc. including all locations detail which are under scope of work. This will help ISA to		Please find the updated clause in the Corrigendum 1

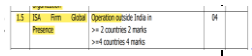
Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
				understand the overall coverage of scope and can propose best solution to GMDC.		
42	Page 19	Section 5: Scope of work- Phase I	Activities of Phase I (Sr. 01 & 02)	We understood that all the detail will be available at central locations to carry out the Activities under Phase I. In case of any site visits to be done, please provide the clarity for the same on how many site visits to be done & locations of site visit.		Site visits needs to be done to collect the information as information of some IOT including surveillance cameras etc. is not Connected Centrally at HO ISA to consider the travel, boarding, lodging and manday costs for the same.
43	Page 20	Section 5 : Scope of work- Phase II	Activities under Phase II (Sr. 3.1 to 3.7)	We understood that PT activities will be carried out from centrally. Please clarify: Is there any site visit to be done during activities to be performed under Phase II? If any site visits to be done, please provide the clarity for the no. of locations & other details where Phase II activity to be performed onsite.		Site visits needs to be done to collect the information as information of some IOT including surveillance cameras etc. is not Connected Centrally at HO ISA to consider the travel, boarding, lodging and manday costs for the same.
44	Page 20-21	Section 5 : Scope of work- Phase III	Activities under Phase III (Sr. no. 5)	Is there any implementation role of ISA? Since this is Audit & Assessment work, we request to remove the Implementation/execution scope from the bid.		This is mentioned in the PMC scope The ISA needs to monitor the implementation and installation works being done by the onboarded bidder

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
45	Page 21	Section 5 : Scope of work - Phase III	Activities under Phase III (Sr. no. 6)	Please clarify:Who will provide all required infrastructure/stationary for Training? Who will bear the Training related cost? Request to define the exact Roles & Responsibility of ISA under this scope		The ISA needs to conduct the offline training for which the travel boarding and lodging expenses of the persons being deputed needs to borne by the ISA All other training costs like stationary location arrangement etc. shall be borne by GMDC.
46	Page 21	Section 5: Scope of work - Phase IV	Activities under Phase III (Sr. no. 7)	Hope ISA is responsible to carry out VAPT for two instances (In Phase II & IV). In Phase IV, it is to be done only once. If still any gap found, ISA will not responsible for carry out said activities again. In case of re-carry out activity in Phase IV, ISA will be paid additional cost as per agreement & as per price quoted for Phase IV. Please clarify		Yes, the interpretation is correct. Post the second assessment ISA needs to ensure compliance thru implementation and installation monitoring and conducting tests for Acceptance Testing. During PMC stage while conducting AT if the ISA feels the need to Assessment they should consider the cost of the same in PMC part
47	Page 21	Section 5: Scope of work - Phase IV	Activities under Phase III (Sr. no. 8)	Please provide the more clarity on Compromise Assessment to be done by ISA. What is the final objective expected by GMDC through this Audit. This will enable us to understand the your requirement and help us to design the solution accordingly under this scope.		The broader scope is defined on page no. 55 in the Technical specification section Please offer the cost based on the same

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
48	Page 21	Section 5: Scope of work - Phase IV	Activities under Phase III (Sr. no. 9)	Request to remove the scope.		No change. As Per RFP Scope and T&C
49	Page 21	Section 5: Scope of work - Phase IV	Activities under Phase III (Sr. no. 11)	Please provide detailed scope of ISA under said Mock drill activity.		No change. As Per RFP Scope and T&C
50	Page 21	Section 5: Scope of work - Phase V	Activities under Phase III (Sr. no. 13)	It is understood that ISA will be responsible to assist/support GMDC for Compliance Certificate process. Also, how many locations to be covered for said Compliance Certificate. Please provide all locations detail. All the cost of Certification to be born by GMDC .Please correct if this understanding is not right.		Location details available in RFP Assistance, Documentation, Policy formulation and Compliance post policy implementations are to be managed by the ISA. The audit and certification charges will be borne by GMDC
51	Page 22	Section 6 Pre qualification criteria	4. Experience of Executing similar works associated to VAPT, Gap Analysis, Cybersecurity architecture Design, Cyber Security Policy Framework design, Compliance certification domain expertise and training management for cybersecurity in Government, PSUs and Corporates in India within the last three yearsOne project of similar nature costing not less than 5 Cr	Are all the experience criteria to be covered in single work order? Since it is challenging to have all the criteria in single work order, May we request to modify the clause as under :**Experience of Executing similar works associated with any of the 03 experience criteria from following :- VAPT / Gap Analysis/ Cybersecurity architecture Design / Cyber Security Policy Framework design/ Compliance certification domain expertise / training management for cybersecurity in**		Please find the updated clause in the Corrigendum 1

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
			value of assignment to be awarded	**Government, PSUs and Corporates in India within the last three years**" One project of similar nature costing not less than 5 Cr value of assignment to be awarded OR Two project of similar nature costing not less than 2.5 Cr value of assignment to be avoided. OR mThree project of similar nature costing of 3 Cr value of assignment to be awarded.		
52	Page 22	Section 6 Pre-qualification criteria	4. Supporting to be given against Sr. no. 4Copy of Work Orders / Contracts ANDCopy of Completion certificate from Client along with the copy of purchase Order	In case of Project Completion Certificate not available, Kindly accept the CA certified Payment acknowledgement against said Project as evidence. May we request to modify the clause as under "Copy of Work Orders / Contracts ANDCopy of Completion certificate from Client along with the copy of purchase Order/ CA certified Payment of said Project		Please find the updated clause in the Corrigendum 1
53	Page 22	Section 6 Pre-qualification criteria	5. Financial Capability The ISA should have overall average annual turnover of at least INR 50 Crore in last 3 financial years (FY20-21, FY 21-22, FY 22-23)	Since Audited statement for Year 2022-23 still awaited, request to modify the FY criteria as under: " The ISA should have overall average annual turnover of at least INR XX Crore in any 3 financial years out of last 04 financial year (FY 19-20, FY20-21, FY 21-22, FY 22-23)"		Please find the updated clause in the Corrigendum 1

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
54	Page 22	Section 6 Pre-qualification criteria	5. Financial Capability The ISA should have overall average annual turnover of at least INR 50 Crore in last 3 financial years (FY20-21, FY 21-22, FY 22-23)	Looking to the large coverage and considering the criticality of said project, May we request you to modify the turn over criteria as under :" The ISA should have overall average annual turnover of at least **INR 80** Crore in any 3 financial years out of last 04 financial year (FY 19-20, FY20-21, FY 21-22, FY 22-23)"NOTE: Request to change in Technical marks criteria as well in line with above modification.		No change. As Per RFP Scope and T&C
55	Page 32	Section 7 Instruction to ISAs	Sr. 1.1 under Criteria for evaluation and comparison of technical bids 	Please update the scoring as per our request in Pre-qual criteria above (sr. no.) >= 80 Cr 4 Mark >=90 Cr. 6 Mark >= 100 Cr. 8 Mark		No change. As Per RFP Scope and T&C
56	Page 33	Section 7 Instruction to ISAs	Sr. 1.3 under Criteria for evaluation and comparison of technical bids 	Please update the scoring as per our request in Pre-qual criteria above (sr. no.) >= Purchase orders of similar nature having total value of 5 Cr - 10 Mark >= Purchase orders of similar nature having total value of 10 Cr- 15 Mark >= Purchase orders of similar		Please find the updated details in the RFP

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
				nature having total value of 15 Cr- 20 Mark		
57	Page 33	Section 7 Instruction to ISAs	Sr. no. 1.4 	1. We understood this should be ISO 27001 certificate not ISO 27000 - Pl correct the criteria.2. We request to remove ISO 9000 Quality certificate (since it is not directly relevant with Cyber or current bid scope of work)		These are the Certificate the ISA should have. Please find the updated clause in the Corrigendum 1
58	Page 33	Section 7 Instruction to ISAs		Which evidence to be submitted for this criterion. We understood that self-declaration from Bidder will be considered. Please clarify		You can give the - Registration details of the firms in other countries or address details as mentioned in the website etc.
59	Page 33	Section 7 Instruction to ISAs		Pl provide clarity with respect to Time frame as asked in this criteria (is it 10 years OR 03 years)		Orders executed in last 3 years need to submitted
60	Page 35	Section 7 Instruction to ISAs	GMDC may ask ISA to match L1 prices under each item / head.	Kindly remove this sentence.		No change. As Per RFP Scope and T&C

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
61	Page 44	Section 8 IT Asset Discovery (For existing infrastructure at all locations	GMDC is managing all its IT assets through the tools they are using. - ISA can review the information available in the tool and use the same for further tests associated to assessments etc. - In case the ISA feels that they need the information in their tool then they can conduct the discovery process using their tools	It is understood that all the asset/devices/endpoints/applications/IoT devices/BYOD etc (which are under scope of work) are already discovered and under monitoring of GMDC. Please confirm on the same. Also, request to modify the clause as under:" In case any asset/components not under discovery of GMDC tool, ISA will not responsible for making their discovery/monitoring of said tools. ISA can carry out test based on best available data/information in such cases if possible.		Please find the updated clause in the Corrigendum 1
62	Page 53		Red Team Testing activity post VAPT and implementations of Audit recommendation	It is understood that Implementation of Audit recommendation is out of scope of ISA		Yes, Implementation of Audit recommendations post Gap analysis and report submission will be done by the onboarded bidder who will supply hardware, software as per the architectural recommendations given by the ISA
63	18	SECTION 4	Generic	Could you let us know if the assessments needs to be done centrally or if the visit to the Sites is also required?		The bidder should consider the cost of Site visits in the bids as Components not connected

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
						centrally needs to checked, discovered and assessed.
64	20	SECTION 5	3.1	Could we get detail view on the no of devices and type of devices that needs to be considered for network and infrastructure VAPT		Please find the updated RFP document and refer the revised Section 4 which will have the details of existing infrastructure with make and model definition and location where it is installed
65	20	SECTION 5	3.2& 3.3	Could we get detail view on no of applications for example (Web based/ ERP/ Website/ Database /APIs/Cloud based application& services) that needs to considered for Vulnerability Assessment and Penetration testing		
66	20	SECTION 5	3.4	Could we get detail view on no of end points that needs to considered for Vulnerability Assessment and Penetration testing		
67	20	SECTION 5	3.5	Could we get detail view on CCTV NVRs/CCTV Servers, Access and Biometric, IP Phones, IP SCADA systems in mines and all IOT devices that that needs to considered for Vulnerability Assessment and Penetration testing		
68	56	SECTION-9	Security Architecture	Is the scope of Security Architecture for the overall IT infrastructure? Or certain Application specific? Kindly Confirm		Bidder must define the Security architecture for all the IT assets including Hardware, Software and API. the architecture should be scalable and align in line with

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
						the digital transformation vision of GMDC
69	56	SECTION-9	Security Architecture	Is OT security architecture review and recommendation part of this scope?		As of now OT is very limited but the solutions being proposed should ensure support for OT security when convergence of OT and IT will happen
70	60	SECTION 11	Audit Compliance Certifications	What is scope ISMS certification readiness assessment for eg no of sites, no of Business units, technology etc that needs to be covered		ISMS need to be done for all sites and it should cover all Business units.
71	22	SECTION 6	5 Financial Capability	FY 22-23 Financial Report may take some more time. Can we provide FY 21-22, 20-21, and 19-20 financials?		Please refer the updated RFP
72	20	SECTION 5	Scope of Work	Could you elaborate the role of of the ISA during the Implementation/Build Phase?		The scope of ISA would be project management during this phase as per the specifications defined. ISA will not do the implementation

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
73	10	Section 1 and Section 5	Section 1 and Section 5	Section 1 has a brief which has mentioned multiple activities under Risk Assessment i.e Cloud Security, Third party, Ransomware Stimulator, Incident Response Readiness, and VAPTSection 5 - SOW has given Phase 1 followingReview of IT Assets discovered and managed by GMDC through the appropriate tools.Post review if the ISA feels the needs of asset discovery in their tools then they can do the same or else use GMDC's data available in their toolSecurity Hardening (Policy review and Assessment) **Question1. Do we need to perform individual assessments or has to be part of Risk Assessment - Cloud Security, Third party, Ransomware Stimulator, Incident Response Readiness and 2. Section 5, phase 1 gives specific requirement on IT asset discovery and security hardening, which doesn't align with what has been asked in Section 2 Brief of Risk Assessment**		Section 2 is just the introduction and we have defined the broad scope of assessment for the reference of the bidder. That has no association with the Scope of work All assessment needs to be performed as per the definition given in Scope of Work as per the technical specifications defined.

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
74	10	Section 1 and Section5	Section 1 and Section 5	**Question**Do we need to use the existing defined GMDC control framework, methodology, and approach to perform assessments, if yes then provide some details and no then what are the expected standard, framework, etc		Please find the updated clause in the Corrigendum 1
75		Section 4	DETAILS OF EXISTING LOCATIONS, USERS AND IT INFRASTRUCTURE	Kindly provide following Internal IP's External IP's No of Routers No of Database Virtualization Technology No of API No of Web Application Details on Security Devices/Solution like SIEM, FIM, DLP, WAF Confirm on Total no of Servers since currently only ERP Servers - 3 and Rack Server 1, but there are more then 5 applications Just like Head office do we need to assess Branch Location, if yes provide details		Please find the updated clause in the Corrigendum 1

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
76	33	Section 7Criteria for evaluation and comparison of technical bids.	1.2	1.2No. of Certified Personals for Cyber security services as per the PQ.**Questions:**What artifacts need to be submitted to satisfy these conditions if we have more than 100 personnel's		Please refer Annexure VIII which has the format for the same.The same should be submitted by the ISA on its letter head and duly signed by the HR department authority
77	33	Section 7 Criteria for evaluation and comparison of technical bids.	1.3	**1.3** Experience of Executing similar works associated to VAPT, Gap Analysis, Cybersecurity architecture Design, Cyber Security Policy Framework design, Compliance certification domain expertise and training management for cybersecurity in Government, PSUs and Corporates in India within the last three years **Question** 1. Can we expect some relief in Value and till what price, e.g from 5cr can we expect till 1cr or 2cr 2. Can we combine multiple clients PO with similar work experience and aligning with GMDC SOW 3. We are global company, can we share our experience, expertise		Please find the updated clause in the Corrigendum 1

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
				and execution with similar SOW for client outside India		
78	33	Section 7Criteria for evaluation and comparison of technical bids.	1.5	1.5 ISA Firm Global Presence**Question**What artifacts need to be submitted to satisfy these conditions if we are present in more then 4 countries		You can give the - Registration details of the firms in other countries or address details as mentioned in the website etc.
79	33	Section 7 Criteria for evaluation and comparison of technical bids.	1.6	1.6 ISA's domain expertise in Government and PSU Vertical Questions What artifacts need to be submitted		Supporting Purchase order and completion certificates
80	35	Section 7 Criteria for evaluation and comparison of technical bids.	Choice of Firm	Kindly elaborate on "GMDC may ask ISA to match L1 prices under each item / head."		Please find the updated clause in the Corrigendum 1

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
81	42	Section 7Criteria for evaluation and comparison of technical bids.	Software licenses (wherever applicable)	The ISA shall be responsible for providing Software (System Software, Application Software, Device Drivers, IOS, etc.) required, if any, to meet any additional requirements during the currency of the Agreement without any additional cost to GMDC. All license software must be in the name of GMDC. The ownership of any customized software involved will be of the GMDC.**Question1. Kindly elaborate what are the approx. cost of this software's 2. What about Timelines3. What about resources**		Please find the updated clause in the Corrigendum 1
82	42	Section 7 Criteria for evaluation and comparison of technical bids.	Installation of additional hardware (wherever applicable)	During the currency of the Agreement, for any additional requirement of equipment including interface equipment, the specifications will be provided by the ISA. GMDC/The Third-Party Agency will verify suitability of the specifications submitted by ISA and recommend to GMDC for acceptance. The ISA will be obligated to undertake integration, operation and maintenance for all additional equipment if required. Question 1. Kindly elaborate what are the		Please find the updated clause in the Corrigendum 1

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
				approx cost of this 2. What about Timelines 3. What about resources		
83	42	Section 7Criteria for evaluation and comparison of technical bids.	Support from external agency (if applicable)	In case, if ISA wish to have support from any external agency, it's necessary to inform GMDC in written prior to allow them to work on GMDC infrastructure. The information should contain all respective information about the company from whom support has been extended, the person/group of people and the segment in which services has been taken. On completion of the task, another report should be submitted by mentioning action taken by this person/group of people from external agency, with duration. The ISA is sole responsible for the action taken by such agency on their behalf. No Data/ Information should be sent out of the premise without obtaining prior written confirmation from the GMDC.**Questions:**1. How it's different from Sub-contracting2. Incase if its needed, at what stage ISA can do this, before selection, after, mid, etc.		Clause Stand Deleted. No Subcontracting is Allowed. Please find the updated clause in the Corrigendum 1

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
84	44	Section 11	AUDIT COMPLIANCE CERTIFICATIONS (TO BE INITIATED POST COMPLETION OF AUDITS/CORRECTIONS/DEPLOYEMENT OF ALL HARDWARE AS RECOMMENDED)	Does ISA need to perform ISO 27001 Gap Assessment, Readiness Assessment and Consulting so that GMDC can go for ISO 27001 Certification Will ISA represent the GMDC during ISO Certification audit and if yes what are the timelines		Yes ISA will represent GMDC during the ISO Certification
85	63	Section 12	UNPRICED BOQ FOR TECHNICAL DETAILS OF TOOLS, MANPOWER DETAILS	Details of Tools that will be used**QuestionWhat kind of tools currently GMDC uses, can we use the same during the tenure**		GMDC is not using any tools as of now.ISA to provide details of the tools / software being used while performing the assessment activity.
86	76	Annexure VI	Work Experience details -as mentioned in the Pre-qualification criteria	Can we share email or any other artifacts where we don't have a "Completion Certificate", also provide alternative of completion certificate		Yes Email from the Clients authorized Signatory can be considered as completion certificate

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
87	20	1	Review of IT Assets discovered and managed by GMDC through the appropriate tools. Post review if the ISA feels the needs of asset discovery in their tools then they can do the same or else use GMDC's data available in their tool	Should we use the GMDC Asset discovery tool or our own tool? Kindly furnish a comprehensive list of all assets. share us the vendor name which are included for review. The RFP indicates that this list pertains exclusively to the Head office. Is the assessment exclusively targeted at the Head office, or are other locations also within scope? If other locations are included, please share an inventory list that necessitates inclusion.		Please find the updated clause in the Corrigendum 1
88	20	2	Security Hardening (Policy review and Assessment)	Please provide a complete list of all devices along with vendor name that need to be reviewed.		
Phase 2						
89	20	3.1	Vulnerability assessment and Penetration Testing for Network and Security Infrastructure	Please provide the complete list of the asset details What is the frequency of scan		Minimum Two times - First during Phase II- Second as defined in Phase IV

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
90	20	3.2 & 3.3	Vulnerability assessment and Testing for Application Testing (Web based/ ERP/ Website/ Database /APIs) Vulnerability assessment and Testing for Cloud based services (SAAS/PASS/IAAS)) for all hosted applications working in Cloud. Define the parameters and ways to check applications hosted in the cloud using SAAS model	Please provide the complete list of the asset details What is the frequency of scan Should we conduct a single VAPT (Vulnerability Assessment and Penetration Testing) for various aspects Web-based systems, ERP, APIs, SAAS, PASS, IAAS etc Or do we need to perform separate VA and PT tests for devices? If separate tests are necessary, could you specify which devices should be tested together and which ones should be tested separately? Please indicate the nature of the software application. Is it a web-based application, a mobile application, or a thick client application? If the application falls under the categories of mobile or thick client, please provide information about the platform it is intended to run on. Do you have a preference between grey box testing and black box testing?		As above Testing should done as per the Specifications defined Specifications 8 and SoW in Section 5 Refer Section 4 for details Testing should be done as per the scope of work and specifications mentioned in the tender

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
91	20	3.4.	Vulnerability assessment and Testing of End Points (Desktops/Laptops/Tablets /BYOD devices getting connected to the network)	Please furnish the complete count of assets required for conducting the assessment.Additionally, please clarify whether we should exclusively carry out Vulnerability Assessment or if Penetration Testing is also included.		Count is mentioned in the Priced Bid.ISA to offer the cost as per the total unit defined . Also refer the updated section 4 having quantity details at each location Please find the updates in the Corrigendum 1
92	20	3.5.	Vulnerability assessment and Testing of CCTV NVRs/CCTV Servers, Access and Biometric, IP Phones, IP SCADA systems in mines and all IOT devices getting connected to the network	Please furnish the complete count of OT/IOT devices Please specify the make and model Kindly elucidate whether we are to solely conduct a Vulnerability Assessment, or if Penetration Testing is also encompassed.		Count is mentioned in the Priced Bid. ISA to offer the cost as per the total unit defined Also refer the updated section 4 having quantity details at each location Please find the updates in the Corrigendum 1
93	20	3.6	Vulnerability Assessment and PET if required for indoor wireless solutions at Head Office and RF Links installed in mines	How may wireless solutions are present in the environment? Kindly furnish with a complete list with make and model details. For how many locations, do we need to perform assessment? Please specify the location/sites. Additionally, specify SSID for each location		Please find the updates in the Corrigendum 1 and refer the revised Section 4 which will have the details of existing infrastructure with make and model definition and location where it is installed

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
94	20	3.7.	Assessment for Security gaps and enhancement recommendation for Microsoft 365 Email solutions being used by GMDC	What is the total number of mailboxes		Please find the updates in the Corrigendum 1 and refer the revised Section 4 which will have the details of existing infrastructure with make and model definition and location where it is installed
95	20	4	Architecture, policy and framework formulation for additional security solutions that includes- Security Architecture design- Information Security Management system design- Security Operation Center design along with Analytics- Disaster recovery (DR) site design- Incident response, Business Continuity and Disaster recovery plan	How many data centres and branch offices or another offices must we take into account? Please furnish the comprehensive list.		Location details are there in Section 4. All the locations need to be covered.
Phase 3						
96	21	6	Primary User Awareness training as per the Training Module designed by the ISA (scheduled offline session to be conducted at all locations)	How many users do we need to consider for training also provide the total number of locations that need to be considered for offline training		All Locations as mentioned in Section 4 needs to be covered for Offline Training.For User Count Refer Section 10 in the updated Corrigendum 1
Phase 4						

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
97	21	10	Red Team testing to check resilience of the complete infrastructure to cyber attacks	Target Information: • Specific systems, applications, or networks to be assessed: • Purpose of the assessment (e.g., infrastructure security, application security, social engineering): • If social engineering/phishing is part of assessment then, can you provide specific email addresses to target?• Any specific goals or scenarios to be tested: • Are there any restrictions or limitations on the scope of the assessment?Rules of Engagement: • What are the rules of engagement for the red team activity? (e.g., no disruption of critical systems, no physical harm): • Are there any specific test scenarios or attack vectors to prioritize or avoid?Additional Information: • Are there any known vulnerabilities or concerns that should be addressed? • Any other relevant details or requirements for the red team activity?• Are there any legal or regulatory considerations that need to be taken into account?• What is the expected timeline for the red teaming engagement?		ISA to define and give the complete process, scenario etc. as per the best industry practices being used for Red Teaming exercises.Tentative timelines are defined ISA to give the actual timelines
98	21	11	Mock Drill for Incident management and Business continuity using DR site	How may DR sites are present in the environment		No DR Site as of Now GMDC will come up with the DR site for

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
						which ISA needs to define the security architecture
Phase 5						
99	21	13	Compliance certification process for ISO 27001 certificate (ISA will remain onboarded till the certificate is issued)	Company background, its business, and geography and expected scope of certification. Business location(s) that need to be covered for compliance IS0 27001 (mention the address Add more rows if needed)		Required Details are mentioned in the RFP along with Scope of work. Please find the updated clause in the Corrigendum 1. All the details as per the requirement will be shared with the onboarded ISA
				Provide the total number of locations that needs to be considered for this assessment.		
				How many employees/contract IT staff are employed at each location? Also explain the IT vendors and their roles		
				Has company got any compliance/process certificate e.g? ISO 9001 ISO 14001 etc.		
				Please briefly describe the IT infrastructure e.g. applications, servers, network etc. and respective location.		
				Explain **IT organization** structure and roles/responsibilities briefly. Any outsourced vendors involved in operations.		
				Do you have IT governance/IT Security/ITSM organization within IT department?		

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
				State the end objective e.g. Customer requirement, internal requirement, ISO certification for process improvement/IT Service improvement etc.		
				What is the timeline for implementing and achieving the certification?		
				Is Application development is carried out in-house or outsourced? Briefly list main applications that is developed in-house.		
				Are IT services clearly documented and SLA is monitored? Do you have IT helpdesk in place? Pl explain the tools if used any		
				What types are IT audits are currently being carried out and the scope and frequency of such audits – Internal/External		
				How IT asset including software assets management is carried out? Please mention the tools if used any.		
				State the local Legislative/ Regulatory compliances that has to be fulfilled.		
				Please provide any publicly available information relating to your organization and information security management. i.e. your		

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
				website or any social media presence		
				Brief description of the level of security control you require.		
				State any other requirements that has to be fulfilled, other than achieving the ISO 27001 certification.		
SECTION 6 – PRE-QUALIFICATION CRITERIAS						
100	22	4	Experience of Executing similar works associated to VAPT, Gap Analysis, Cybersecurity architecture Design, Cyber Security Policy Framework design, Compliance certification domain expertise and training management for cybersecurity in Government, PSUs and Corporates in India within the last three years One project of similar nature costing not less than 5 Cr value of assignment to be awarded.	We request you to please amend this to - One project of similar nature costing not less than 1.5 Cr value of assignment to be awarded.		Please find the updated clause in the Corrigendum 1

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
101	64	2.5	Vulnerability assessment and Testing of IOT Endpoints (CCTV NVRs/CCTV Servers Access and Biometric, IP Phones, IP SCADA systems in mines and all IOT devices getting connected to the network)	Can align some partner to do this piece of Scope.		No Subcontracting or Joint Venture is allowed.
102	23	7	- 07 Certified (CISA or equivalent & OSCP or equivalent) cyber security audit professional for audits networks, applications, websites, IOT devices and other	We request you to please amend this to - 02 Certified (CISA or equivalent & OSCP or equivalent) cyber security audit professional for audits networks, applications, websites, IOT devices and other		No change . As Per RFP Scope and T&C
103	Page: 18	SECTION 4- DETAILS OF EXISTING LOCATIONS, USERS AND ITINFRASTRUCTURE	GMDC offices are located at Ahmedabad and other locations as mentioned below. Of the total locations mentioned in the above BOQ	Certification for ISO 27001:2022 be covered across all locations or only Head Office		All Locations of GMDC
104	Page: 18	SECTION 4- DETAILS OF EXISTING LOCATIONS, USERS AND IT INFRASTRUCTURE	GMDC offices are located at Ahmedabad and other locations as mentioned below. Of the total locations mentioned in the above BOQ	Are the Operations and Data centralized?		Only ERP and mailing is centralized. Rest all resources are De centralized

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
105	Page: 21 & 59	SECTION -10 USER TRAINING FOR CYBERSECURITY AWARENESS, POLICY IMPLEMENTATIONSECTION -5 Scope of Work Phase III & Phase IV	SECTION -10 USER TRAINING FOR CYBERSECURITY AWARENESS, POLICY IMPLEMENTATIONSECTION -5 Scope of Work Phase III & Phase IVPrimary User Awareness training as per the Training Module designed by the ISA (scheduled offline session to be conducted at all locations)Publishing of complete ISMS policy post management approval and user training for creating awareness	No. of users for the training as specified in the below areas.		Refer the updated details in Section 10 of the RFP Please find the updated clause in the Corrigendum 1

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
106	Page: 21 & 60	SECTION -10 USER TRAINING FOR CYBERSECURITY AWARENESS, POLICY IMPLEMENTATIONS ECTION -5 Scope of Work Phase III & Phase IV	SECTION -10 USER TRAINING FOR CYBERSECURITY AWARENESS, POLICY IMPLEMENTATIONSECTION -5 Scope of Work Phase III & Phase IVPrimary User Awareness training as per the Training Module designed by the ISA (scheduled offline session to be conducted at all locations)Publishing of complete ISMS policy post management approval and user training for creating awareness	Are virtual Sessions for training acceptable?		No

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
107	Page: 44	SECTION – 8 SPECIFICATIONS AND PROCESS DEFINITIONS FOR TASK DEFINED IN SOCOPE OF WORK	IT Asset Discovery (For existing infrastructure at all locations)GMDC is managing all its IT assets through the tools they are using. - ISA can review the information available in the tool and use the same for further tests associated to assessments etc.	Which are the tools used currently?		Please find the updated clause in the Corrigendum 1
108	Page: 21	PHASE V	Compliance certification process for ISO 27001 certificate (ISA will remain onboarded till the certificate is issued)	Which Teams/Team members will be aligned from GMDC to support for preparation for Audit process and implementation of ISO 27001 standards?		Will share the details with the Onboarded ISA
109	Page: 22	SECTION 6 – PRE-QUALIFICATION CRITERIAS	Experience of Executing similar works associated to VAPT, Gap Analysis, Cybersecurity architecture Design, Cyber Security Policy Framework design, Compliance certification domain expertise and training management for cybersecurity in Government, PSUs and	Please relax this criteria for MSME / NSIC firms based on capability		Please find the updated clause in the Corrigendum 1

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
			Corporates in India within the last three year			
110	Page: 22	SECTION 6 – PRE-QUALIFICATION CRITERIAS	The ISA should have overall average annual turnover of at least INR 50 Crore in last 3 financial years (FY20-21, FY 21-22, FY 22-23).The revenues of 50 Cr should be from the service revenue generated from services associated to cyber security audits and security architecture designs	Certificate(s) from statutory auditor with all relevant details from the ISA. The ISA shall provide a copy of each of audited annual report to ascertain its turnover & net-worth.		Please find the updated clause in the Corrigendum 1
111	Page: 22	SECTION 6 – PRE-QUALIFICATION CRITERIAS	ISA should be a legal entity registered in India, since last 10 (Ten) years under either Indian Companies Act 1956/2013 or LLP Act 2008	please relax this to 07 years instead of 10		No change. As Per RFP Scope and T&C

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
112	Page: 22	SECTION 6 – PRE-QUALIFICATION CRITERIAS	The ISA should have the Empanelment of its firm with the CERT -IN	Please relax this criterion for MSME / NSIC firms based on capability		No change. As Per RFP Scope and T&C
113	general	general	Pre-Bid Meeting: Pre-Bid Meeting will be held on 01/09/2023 at 15.00 Hours. Venue of pre-bid meeting will be Corporate Office, GMDC, Ahmedabad (Gujarat). Maximum two members per Bidder will be allowed for the Pre-Bid meeting.	Please provide link for online attending the meeting		Online meeting link published and conducted.
114	22	**Section-6, Clause(1)** (Pre-Qualification Criteria's) **LEGAL ENTITY**	**Clause No. 6(1)** ISA should be a legal entity registered in India, since last 10 (Ten) years under either Indian Companies Act 1956/2013 or LLP Act 2008.	Request to modify the clause as below: **ISA /Consortium/Joint Ventures** should be a legal entity registered in India, since last **05 (Five) years** under either Indian Companies Act 1956/2013 or LLP Act 2008.	-	No change. As Per RFP Scope and T&C

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
115	22	**Section-6, Clause(4)** Pre-Qualification Criteria's	**<u>Clause No. 6(4)</u> Experience of Executing similar works associated to VAPT, Gap Analysis, Cybersecurity architecture Design, Cyber Security Policy Framework design, Compliance certification domain expertise and training management for cybersecurity in Government, PSUs and Corporates in India within the last three years.** One project of similar nature costing not less than 5 Cr value of assignment to be awarded	Hence, request to modify the clause as below: One project of similar nature /IT Project costing not **less than 20 lakhs** value of assignment to be awarded	The existing clause is restrictive and binding in nature. The work purely related to Cyber Security Policy Framework, VAPT, Compliance certification in Government/ PSU/ Corporate of 5 crore has not be provided till now. Also, as per the MEITY Guidance notes, the experience of consultant firm shall be around 1/5 times the work to be awarded (assuming the cost of SoW around 1 Cr).	Please find the updated clause in the Corrigendum 1

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
116	23	**Section-6, Clause (5)** (Pre-Qualification Criteria's) **FINANCIAL CAPABILITY**	**Clause No. 6(5)**The ISA should have overall average annual turnover of at least INR 50 Crore in last 3 financial years (FY20-21, FY 21-22, FY 22-23).**The revenues of 50 Cr should be from the service revenue generated from services associated to cyber security audits and security architecture designs**	Hence, request to modify the clause as below:The **ISA/Consortium/Joint Venture** should have overall average annual turnover of at least INR **5** Crore in last 3 financial years (FY 2020-21 to 2021- 2022 **(as per the last published audited balance sheets) AND FY 2022-23 (as per Provisional Certificate)The revenues of 10 Cr should be from the service revenue generated from services associated to consultancy/advisory/audit related to IT/ ICT**	The existing clause is restrictive and binding in nature. Also, as per the MEITY Guidance notes, the turnover of consultant firm shall be around 5 times the work to be awarded (assuming the cost of SoW around 1 Cr).	Please find the updated clause in the Corrigendum 1
117	24	**Section-6, Clause(7)** (Pre-Qualification Criteria's) C**ERTIFIED MANPOWER**	**Clause No. 6(7)**The ISA should have the following certified manpower onboard 1. 07 Certified (CISA or equivalent& OSCP or equivalent) cyber security audit professional for audits networks, applications, websites, IOT devices and other 2. 03 Certified (CEH or equivalent) professional associated to domain expertise in Ethical Hacking practices for conducting tests like Red Team, Compromise assessment etc.3. 03 Certified (CISSP-	Request to modify the clause as below:The **ISA/Consortium/Joint Ventures** should have the following certified manpower onboard (combined)1. **02 Certified (CISA/ CEH/ CISSP or equivalent or OSCP or equivalent/AWS/CCNA**) cyber security audit professional for audits networks, applications, websites, IOT devices and other 2. **01 Training experts** for conducting cyber security training 3. **01 Certified** (ISO 27000 LA or equivalent) Compliance certification experts for handling ISO27001 certification process4. **01 Project management Certified** professional (PMP or equivalent	The existing clause is restrictive and binding in nature. Having both CISA & OSCP certification for the resource performing audit, is not mandatory as either certification provides necessary knowledge for entire scope of audit.	No Change. As per RFP T&C

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
			ISSAP or equivalent) Design experts associated to security architecture design4. 02 Training experts for conducting cyber security training 5. 02 Certified (ISO 27000 LA or equivalent) Compliance certification experts for handling ISO27001 certification process6. 02 Project management professional 7. 02 Certified (PMP or equivalent with Security project handling experience) Project Professionals for managing the projects 8. 01 Documentation expert for draft documents like policy frame work etc.	with Security project handling experience) 6. **01 Documentation expert** for draft documents like policy frame work etc.**.**		
118	2427	**Section-6, Clause(8)**(Pre-Qualification Criteria's) Section 7INSTRUCTION TO ISAs	**Clause No. 6(8)**The ISA should have the Empanelment of its firm with the CERT -IN**Consortium / Joint Venture:**Consortium / Joint Venture are not allowed.	Request to kindly modify clause as below:The ISA should have the Empanelment of its firm with the CERT -IN.**Incase of consortium/JV, the Lead Bidder should have the Empanelment of its firm with the CERT-IN and member/partner, should have applied for CERT-In empanelment as on 31st August 2023.**	The existing clause is restrictive and binding in nature.	No Change. As per RFP T&C

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
119	32	**Section-7, Clause(1) Instruction to the ISAs** (Organizational Strength: Turnover and Employee Strength;Implementation References & Certifications)	**Clause No.1(1.1),**Average Annual Turnover (As mentioned in the PQ section revenue earned from Cybersecurity services will be considered) of the ISA 1. > = 50 Crores as per the PQ req.-- 4 (Max Marks) 2. > = 65 Crores as per the PQ req.-- 6 (Max Marks)3. > = 80 Crores as per the PQ req.-- 8 (Max Marks)	Request to modify the clause as below: Average Annual Turnover (As mentioned in the PQ section revenue earned from **consultancy/advisory/audit related to IT/ ICT** will be considered) of the ISA/Consortium/Joint Ventures 1. **> = 5** Crores as per the PQ req.-- 4 (Max Marks) 2. **> = 15** Crores as per the PQ req.-- 6 (Max Marks)3. **> = 25** Crores as per the PQ req.-- 8 (Max Marks)	The existing clause is restrictive and binding in nature.	Please find the updated clause in the Corrigendum 1

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
120	33	**Section-7, Clause(1) Instruction to the ISAs** (Organizational Strength: Turnover and Employee Strength;Implementation References & Certifications)	**Clause No.1(1.2),**No. of Certified Personals for Cyber security services as per the PQ. 1. > = 20 Employees in security domain ---3 (Max Marks)2. > = 60 Employees in security domain----5 (Max Marks)3. > = 100 Employees in security domain---7 (Max Marks)	Request to modify the clause as belowCombined no. of Certified Personals for Cyber security services/Advisory/Consulting Services as per the PQ.1. **> = 30** Employees in security domain/IT domain ---3 (Max Marks)2. **> = 40** Employees in security domain/IT domain----5 (Max Marks)3. **> = 50** Employees in security domain/IT domain ---7 (Max Marks)	The existing clause is restrictive and binding in nature.	Please find the updated clause in the Corrigendum 1
121	33	**Section-7, Clause(1) Instruction to the ISAs** (Organizational Strength: Turnover and Employee Strength;Implementation Reference	**Clause No.1(1.3),**Experience of Executing similar works associated to VAPT, Gap Analysis, Cybersecurity architecture Design, Cyber Security Policy Framework design, Compliance certification domain expertise and training management for cybersecurity in Government, PSUs and Corporates in India within the last three years.	Request to modify the clause as below: Experience of Executing **similar works/IT Projects in India/Global** within the last three years.1. **> = 1** Purchase orders of similar nature and value not less than 20 Lacs --10 (Max Marks)2. **> = 3** Purchase orders of similar nature and value not less than 20 Lacs--15 (Max Marks)3. **> = 5** Purchase orders of similar nature and value not less than 20 Lacs--20 (Max Marks)	The existing clause is restrictive and binding in nature. As per the MEITY Guidance notes, the experience of consultant firm shall be around 1/5 times the work to be awarded (assuming the cost of SoW around 1 Cr).	Please find the updated clause in the Corrigendum 1

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
		s & Certificati ons)	1. > = 1 Purchase orders of similar nature and value not less than 5 Cr --10 (Max Marks)2. > = 10 Purchase orders of similar nature and value not less than 5Cr --15 (Max Marks)3. > = 20 Purchase orders of similar nature and value not less than5Cr --20 (Max Marks)			
122	33	**Section-7, Clause(1) Instructio n to the ISAs** (Organizat ional Strength: Turnover and Employee Strength;I mplement ation Reference s & Certificati ons)	**Clause No.1(1.6),**ISA's domain expertise in Government and PSU Vertical 1. >= 10 order in the time frame defined in the PQ section -----05 (Max Marks)2. >= 20 order in the time frame defined in the PQ section -------10 (Max Marks)3. >= 30 order in the time frame defined in the PQ section -------15 (Max Marks)	Request to modify the clause as below: **ISA's/Consortium/Joint Venture**s domain expertise in **Government/Private** and PSU Vertical 1. >= 02 order in the time frame defined in the PQ section -------05 (Max Marks)2. >= 04 order in the time frame defined in the PQ section -------10 (Max Marks)3. >= 06 order in the time frame defined in the PQ section -------15 (Max Marks)	The existing clause is restrictive and binding in nature.	Please find the updated clause in the Corrigendum 1

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
123	41	Project implementation	The ISA shall provide, log analysis and other associated training required to monitor the security infrastructure to GMDC Personnel at no cost to GMDC. The training schedule, content and modalities will be defined jointly by both the parties. If Certification is required ISA should consider the training costs to train 04 GMDC team members for the same.	It is required to remove this clause	Since the scope of work requires assessment of infrastructure and audit, the scope of log monitoring and analysis shall not be in the scope of ISA. Further, ISA can impart their knowledge in monitoring/analysis, but certification shall be in the scope of operator of the devices/tools/software etc.	Here we are talking of GDMC personal Certification and training for log analysis needs to be provided to GMDC personal The ISA doesn't have to do the log analysis.
124	76	Annexure VI Work Experience details - as mentioned in the Pre-qualification criteria	Supporting PO and Completion Certificate attached or not	Request to modify the clause as below: Supporting PO or Completion Certificate attached or not	-	No Change. As per RFP T&C
Additional Clauses for inclusion						

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
125	Indemnity			Tenderer shall indemnify and hold harmless the bidder for all Losses incurred in connection with any third-party Claim, except to the extent finally judicially determined to have resulted primarily from the fraud or bad faith of such Bidder.		No Change
126	Limitation of the Bidder's Liability towards the Purchaser			Tenderer (and any others for whom Services are provided) shall not recover from the Supplier, in contract or tort, under statute or otherwise, any amount with respect to loss of profit, data or goodwill, or any other consequential, incidental, indirect, punitive, or special damages in connection with claims arising out of this Agreement or otherwise relating to the Services, whether the likelihood of such loss or damage was contemplated. Tenderer (and any others for whom Services are provided) shall not recover from the Supplier, in contract or tort, including indemnification obligations under this contract, under statute or otherwise, aggregate damages in excess of the fees actually paid for the Services that directly caused the loss in connection with claims arising out of this Agreement or otherwise relating to the Services		Already defined in Section 7

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
127	Non-solicitation			Bidder shall not hire employees of Tenderer or solicit or accept solicitation (either directly, indirectly, or through a third party) from employees of Tenderer directly involved in this contract during the period of the contract and one year thereafter.		No Change
128	Force Majeure			1) Bidder shall not be liable for forfeiture of its performance security, Liquidated damages or termination for default, if any to the extent that its delay in performance or other failure to perform its obligations under the contract is the result of an event of Force Majeure.2) For purposes of this Clause, "Force Majeure" means an event explicitly beyond the reasonable control of the Contractor and not involving the contractor's fault or negligence and not foreseeable. Such events may be due to or as a result of or caused by act of God, wars, insurrections, riots, earth quake and fire, revolutions, civil commotion, floods, epidemics, quarantine restrictions, trade embargos, declared general strikes in relevant industries, satellite failure, act of Govt. of India, events not foreseeable but does not		Already defined in Section 7

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
				include any fault or negligence or carelessness on the part of the parties, resulting in such a situation. In the event of any such intervening Force Majeure, either party shall notify the other in writing of such circumstances or the cause thereof immediately within five calendar days.3) Unless otherwise directed by Tenderer in writing, the selected contractor shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.4) In such a case the time for performance shall be extended by a period(s) not less than duration of such delay. If the duration of delay continues beyond a period of three months, Tenderer and the bidder shall hold consultations in an endeavour to find a solution to the problem.5) Notwithstanding above, the decision of Tenderer shall be final and binding on the bidder regarding termination of contract or otherwise		

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
129	Termination for Convenience			1) In case of termination, Tenderer shall pay the bidder for all work-in progress, Services already performed, and expenses incurred by the bidder up to and including the effective date of the termination of this Agreement.2) Tenderer shall be entitled to terminate/cancel the purchase order at any time for the balance order quantity which is within the delivery schedule with no liability on either side and without assigning any reason thereof. However, the purchase order for the quantity which has already been offered for inspection shall not be cancelled and supply of the same shall be availed in due course of time. 3) Bidder may terminate/cancel the contract by giving a written notice of 30 days in case:a) Its invoices are not paid on timeb) If Tenderer fails to comply with the terms of agreement		Already defined in Section 7

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
130	Retention of copies			On payment of all bidder fees in connection with the Contract, Tenderer shall obtain a non-exclusive license to use within its internal business, subject to the other provisions of this Contract, any Deliverables or work product for the purpose for which the Deliverables or work product were supplied. bidder retains all rights in the Deliverables and work product, and in any software, materials, know-how and/or methodologies that bidder may use or develop in connection with the Contract.		No Change. As per RFP T&C
131	Non-Exclusivity			It is agreed that the services are being rendered on a non-exclusive basis and the bidder shall have the right to pursue business opportunities that it may in its sole discretion deem appropriate.		No Change. As per RFP T&C
132	20	Section 5 - Scope of Work - Phase I	Review of IT Assets discovered and managed by GMDC through the appropriate tools. Post review if the ISA feels the needs of asset discovery in their tools then they can do the same or else use GMDC's data available in their tool	1. Please clarify the expectation on this task 2. Please suggest if asset discovery needs to be performed as part of the assessment		Please find the updated clause in the Corrigendum 1

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
133	20	Section 5 - Scope of Work - Phase I	Security Hardening (Policy review and Assessment)	1. Please confirm if device configuration review is expected as part of this activity. If yes, please provide the type of devices such as servers, routers, firewalls etc. along with their count. 2. Considering that ISMS is already outlined, please suggest what is expected from policy review standpoint		Please find the updated clause in the Corrigendum 1 and refer the revised Section 4 which will have the details of existing infrastructure with make and model definition and location where it is installed. Configuration review is part of the scope. Scope of review and expectations are mentioned in the RFP.
134	20	Section 5 - Scope of Work - Phase II	Vulnerability assessment and Penetration Testing for Network and Security Infrastructure	1. Please confirm if the scope comprises of device IP addresses mentioned under "SECTION 4- DETAILS OF EXISTING LOCATIONS, USERS AND IT INFRASTRUCTURE".2. Confirm if count of internal and external IP addresses as part of the scope3. Confirm the locations which needs to be covered as part of internal VAPT and if the assessment can be performed remotely or over the VPN4. Please confirm if the configuration needs to be reviewed for the in-scope devices or if only Network VAPT needs to be conducted		Please find the updated clause in the Corrigendum 1 and refer the revised Section 4 which will have the details of existing infrastructure with make and model definition and location where it is installed

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
135	20	Section 5 - Scope of Work - Phase II	Vulnerability assessment and Testing for Application Testing (Web based/ ERP/ Website/ Database /APIs)	1. Please provide the count of internal and external applications 2. Confirm if any mobile application needs to be assessed. If yes, please confirm the number of android and ios applications 3. Please confirm whether the applications are critical or non-critical. 4. No. of Functional modules/portals present in the mentioned Applications. 5. What shall be the mode of testing, will it be black box or grey box 6. Please confirm the location which needs to be covered to perform the on-premise application audit 7. Please confirm the number of API that needs to be assessed		Please find the updated clause in the Corrigendum 1 and refer the revised Section 4 which will have the details of existing infrastructure with make and model definition and location where it is installed

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
136	20	Section 5 - Scope of Work - Phase II	Vulnerability assessment and Testing for Cloud based services (SAAS/PASS/IAAS)) for all hosted applications working in Cloud. Define the parameters and ways to check applications hosted in the cloud using SAAS model	1. Please apprise which cloud service provider is currently providing the cloud services.2. Please confirm the count of cloud applications and if they are in-addition to the application testing activity (point 4)3. Apart from application testing, please confirm what is expected as part of cloud review		Please find the updated clause in the Corrigendum 1 and refer the revised Section 4 which will have the details of existing infrastructure with make and model definition and location where it is installed
137	20	Section 5 - Scope of Work - Phase II	Vulnerability assessment and Testing of End Points (Desktops/Laptops/Tablets /BYOD devices getting connected to the network)	1. It is understood that 600 endpoints needs to assessed for VAPT. Please confirm if understanding is aligned with yours. 2. Please confirm that is the objective and expectation from the endpoint VAPT. 3. Please apprise if endpoint OS configuration review also needs to be performed		Number provided is total number of Desktops. ISA is expected to do Sample survey of the different types of endpoints. If need is justified GMDC may go for VAPT assessment of all the devices.
138	20	Section 5 - Scope of Work - Phase II	Vulnerability assessment and Testing of CCTV NVRs/CCTV Servers, Access and Biometric, IP Phones, IP SCADA systems in mines and all IOT devices getting connected to the network	1. Please confirm what is the objective and what is expected as part of the following activities-a) CCTC NVRs/CCTV Serversb) Access and biometricc) IP Phonesd) IP Scada system in minese) All IOT devices2. Please update on the number of count and type of IP SCADA systems and IOT devices		Please find the updated RFP document and refer the revised Section 4 which will have the details of existing infrastructure with make and model definition and location where it is installed

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
139	20	Section 5 - Scope of Work - Phase II	Vulnerability Assessment and PET if required for indoor wireless solutions at Head Office and RF Links installed in mines	1. Need more understanding on the task. 2. Please confirm what is expected with this activity		It is security assessment of Wi-Fi installed at HO and security assessment of the RF Radio Links that are working in the mines. Technical specifications for conducting the VAPT are already given in Section 8. Quantitates are defined in Section 4 Existing infrastructure
140	20	Section 5 - Scope of Work - Phase II	Architecture, policy and framework formulation for additional security solutions that includes- Security Architecture design- Information Security Management system design- Security Operation Center design along with Analytics- Disaster recovery (DR) site design- Incident response, Business Continuity and Disaster recovery plan	1. Please confirm on all locations that needs to be covered as part for network architecture review and if the review can be performed remotely or from a single location2. Need more clarity, understanding, objective and expectation on the following tasks- a) - Information Security Management system designb) - Security Operation Center design along with Analyticsc) - Disaster recovery (DR) site designd) - Incident response, e) - Business Continuity and Disaster recovery plan		All Locations needs to be covered. Refer the details specification in Section 9 which list all the details for the scope of work.

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
141	21	Section 5 - Scope of Work - Phase IV	Red Team testing to check resilience of the complete infrastructure to cyber attacks	1. Please confirm if any specific scenario needs to be perform as part of red teaming activity.2. What is the objective and expectation from red teaming activity3. In case of social engineering such as Phishing, please confirm the number of users that needs to be targeted As discussed during the pre-bid meeting, the scenarios for the red team assignment will be discussed in mutual consultation with the bidder and GMDC. Since, the red team assessment and compromise assessment is to be carried out post the onboarding of the system integrator (for which the bidder will assist GMDC in designing of the RFP, including technical and financial evaluation), it is understood that the tools required for the red team and the blue team would be brought in by the System Integrator.		ISA to define and give the complete process, scenario etc. as per the best industry practices being used for Red Teaming exercises.Tool for Red Teaming will be given by the ISA and not by the onboarded System integrator
142	22	Section 5 - Scope of Work - Phase IV	Publishing of complete ISMS policy post management approval and user training for creating awareness	ISMS Readiness is to be done by the bidder as part of Phase V, but policy needs to be approved in Phase IV. Please provide clarity		ISMS polices to be published in Phase IV will be designed and recommended for deployments as per the ISMS certification guidelines . It will be step towards make GMDC ready so that GMDC can apply for Certification

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
143	22	Section 5 - Scope of Work - Phase IV	Digital Forensics Readiness Assessment	As per discussion held during the pre-bid meeting, as the incident response is to be performed by the bidder post onboarding of the system integrator (for which the bidder will assist GMDC in designing of the RFP, including technical and financial evaluation), it is understood that the tools required for assessing the SOC and maturity of the SOC would be brought in by the System Integrator and not a responsibility of the bidder?		Tools will be given by the ISA and assessment will be done by the ISA
144	23	Section 5 - Scope of Work - Phase IV	User Training	For the user training, please clarify if the bidder is required to develop a tool for implementing a comprehensive training module for information cyber security training or the bidder's responsibility would be only limited to the designing of the content. Also please clarify if the bidder is required to deliver training by physically being present at each of the locations specified in the RFP or the training can be delivered remotely from the HO to other locations. The same understanding also needs to be coroborated inthe financial bid format accordingly.		ISA will develop the training tool and the cost associated to design, development, implementation and integration of the same needs to be considered by the ISA in the turnkey costing being offered. The ISA should give the design on the module in the technical details of the presentation to be submitted

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
145	23	Section 5 - Scope of Work - Phase V	Compliance certification process for ISO 27001 certificate (ISA will remain onboarded till the certificate is issued)	Is GMDC already certified in ISO 27001 previously. Are the policy documents available or the bidder is required to design them from scratch and then get it implemented?As per the understanding gained in the pre-bid meeting, it is understood that the Registered Certifying body (RCB) to be onboarded for the ISO 27001 certification shall be the responsibility of GMDC. GMDC shall enter into a contract with the RCB for the purpose of the ISO 27001 certification.		No GMDC is not certified.All co-ordination, processes, documentations, compliances etc that is needs to ISO 27001 will be done by the ISA and post that on recommendation of the ISA GMDC will signoff with the Certificate issuing body who may conducts random check and audits based on the documentation submittedGMDC will pay all the Certification fess and other fees that will be charged by the Certification body
146	23	Section 6-Pre-Qualification Criteria, point 7 sub point 3	Certified Manpower - Point 7 - Eligibility Criteria Sub point 3 - 03 Certified (CISSP-ISSAP or equivalent) Design experts associated to security architecture design	Our submission for this point is to include the below criteria as well: 3 certified resources having the below certification: CISSP-ISSAP/TOGAF/SABSA.		Please find the updated clause in the Corrigendum 1
147	23	Section 6-Pre-Qualification Criteria, Point 7 sub point 4	Certified Manpower - Point 7 - Eligibility Criteria Sub point 4 - 02 Training experts for conducting cyber security training	Is there any specific qualification/certification which is required for the training resources?		The trainer should be certified in Security, Audits and Policy domain as this training needs to be imparted to the users

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
148	23	Section 6-Pre-Qualification Criteria, Point 7 sub point 6 and sub point 7	Certified Manpower - Point 7 - Eligibility Criteria Sub point 6 - 02 Project management professional Sub point 7 - 02 02 Certified (PMP or equivalent with Security project handling experience) Project Professionals for handling the project	Both the sub points indicate the same type of resources. Please provide clarity		Please find the updated clause in the Corrigendum 1
149	24	Section 6-Pre-Qualification Criteria, Point 8	The ISA should have the Empanelment of its firm with the CERT -IN	Considering that the scope of work for the client requires delivery cyber security services, our submission is that the criteria be modified to the below: The bidder should be CERT-IN Empanelled consistently for the last 7 years without a gap.		No Change. As per RFP T&C
150	73	Annexure VII	In Annexure VII, for the Financial Strength of ISA, System Integration Turnover in LACS is specified	Since the scope of work specified in the RFP is with respect to the cyber security consulting related services, we suggest to include cyber security consulting turnover details in the certificate		Revenue should be from Cyber security business is already mention in the PQ section
151	32	Criteria for Evaluation and Comparison of Technical Bids -	Experience of Executing similar works associated to VAPT, Gap Analysis, Cybersecurity architecture Design, Cyber Security Policy Framework design, Compliance certification domain expertise and	We propose the following changes in the given criteria : Experience of Executing similar works associated to VAPT, Gap Analysis, Cybersecurity architecture Design, Cyber Security Policy Framework design, Compliance certification domain expertise and training		Please find the updated clause in the Corrigendum 1

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
		QCBS - Criteria 1.3	training management for cybersecurity in Government, PSUs and Corporates in India within the last three years>=1 Purchase Orders of of similar nature and value not less than 5 Cr - 10 Marks>=10 Purchase Orders of of similar nature and value not less than 5 Cr - 20 Marks> = 20 Purchase orders of similar nature and value not less than 5 Cr - 30 Marks	management for cybersecurity in Government, PSUs and Corporates in India within the last **Four years**>=1 Purchase Orders of similar nature and value not less than 5 Cr - 10 Marks>=2 Purchase Orders of of similar nature and value not less than 5 Cr with 1 purchase order in Central/State Govt entity - 20 Marks> = 3 Purchase orders of similar nature and value not less than 5 Cr with 1 purchase order more than 15 cr in Central/State Govt - 30 MarksIn addition, mutliyear assurance projects with separate POs issued for each year, would they be considered as separate projects?Separate POs issued for the same client in the last 3 years for different types of cyber security services delivered, would that be considered for evaluation in the criteria?**We suggest that a downsizing of the number of cyber security workorders required for gaining maximum marks be taken into consideration by GMDC.**		

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
152	1	Last Date for Submission of Bid	19th September 2023	We request you to extend the timelines for the submission of the bid response by at least 3 weeks from the date of the release of the corrigendum/publishing of the Pre-Bid Queries, keeping in mind the external dependencies such as EMD/BG, Auditor Certificate		Please refer the updated RFP for the new dates Please find the updated clause in the Corrigendum 1
153	35	Choice of Firm	Final Choice of Firm / Firms, to execute this project shall be made based on conformity to technical and operational requirements, time schedule of execution and appropriateness of priced bid from the point of view of cost competitiveness. GMDC, however, will have the discretion to choose to enter into any price negotiations or not. GMDC may ask ISA to match L1 prices under each item / head.	Does this mean that GMDC is planning to onboard more than one bidder to confirm to the scope of work of the RFP?		No only one ISA will be appointed
154	NA	NA	Suggestive	It is suggested to include a criteria on resource qualifications in the TQ Criteria with marks assigned for various certifications being held by the bidder's personnel		Already there in the QCBS table

Sr. No	Bid Page No	Existing Clause No	Existing Clause	Existing Clause Query	Justification for Change	GMDC Response
155	NA	NA	As per the understanding gained during the pre-bid meeting, it is understood that once the initial gap assessment has been performed by the Bidder, the bidder shall design the to-be cyber security posture of GMDC by creating an RFP for the selection of the system integrator to undertake the implementation of the recommendations suggested in Phase I including the security solutions required to be procured by drafting the specifications of the security solutions in the RFP scope of work. Request to confirm if this understanding is correct			Worked needs to be carried out as per the defined phases. Phases are just for reference purposes and bidder can do the work of another phase in a phase as per the agreement of the final execution model accepted by GMDC
156			Number of Log source for SIEM & SOAR solution. Sequretek Percept XDR(SOC) is priced based on log source and not on EPS			No exiting SIEM or SOAR
157			Cybersecurity Assessment 12 Location connectivity issue will this activity require onsite resource.			Site visits should be planned for initial assessment and post asset discovery also if required the ISA needs to do site visit to carry on the assessment activity
158			Sequretek is a MSME Registered, DIPP, 100% make in India Company. We request for Turnover consideration under MSME registered Vendor			Please refer the updated clause in the RFP
159			Shall we request for removal of Bank Guarantee Claus for MSME Registered Vendor			No change
160			Please support on GMDC Vendor registration or empanelment if required. Further update us the submission date.			Not required as of now.
161			Will Managed Security Services P.O valid for Pre-qualification and Technical evaluation against only VAPT order value of 5 Cr.,			If the scope is matching with the details as mentioned in the PQ the same would be acceptable