OIL INDIA LIMITED
(A Government of India Enterprise)
P.O. Duliajan, Pin – 786602
Dist-Dibrugarh, Assam

CORRIGENDUM NO. 2 DATED 11.09.2023

To

BID NO. GEM/2023/B/3804613 dated 09-08-2023 for Hiring of Consultancy services to develop Cybersecurity at OIL.

This Corrigendum is issued to notify the following changes:

1. Extension of dates:

- Last Date of Bid Submission is **03.10.2023 (14:00 Hrs IST)**
- Last Date of Bid Opening is **03.10.2023 (14:30 Hrs IST)**

2. The following document has been newly uploaded in GEM Portal:

- ANNEXURE-I: OIL's response to the queries of Pre-Bid Conference held on 31.08.2023 and 01.09.2023.

All others terms and conditions of the Bid Document remain unchanged. Details can be viewed at www.oil-india.com.

ANNEXURE-I

OIL's response to the queries of Pre-Bid Conference held on 31.08.2023 and 01.09.2023 in Kolkata, India against GEM BID NO. GEM/2023/B/3804613 dated 09.08.2023 for 'Hiring of Consultancy services to develop Cybersecurity at OIL'.

Sl. No.	Section	Tender Clause	Clarification Sought/Recommendations	OIL's Response
1.	PQC/BEC/BRC Clause No. 3.1	The combined value of executing the above experiences under 3.1 i) and ii) should be minimum of Rs. 2,64,04,000.00 (Rupees Two Crore Sixty-Four Lakh Four Thousand) only. However, if the bidder has experience in executing the above experiences [3.1 i) and ii)] together under a single contract, then the value of the contract should be minimum of Rs. 2,64,04,000.00 (Rupees Two Crore Sixty-Four Lakh Four Thousand) only.	Request to amend the clause with work value within 50lacs.	Not acceptable.
2.	PQC/BEC/BRC		Prebid query regarding JV possible for this bid or direct consultancy.	Provision for JV is not acceptable against the tender.
3.	Section-III SOW 7.1.3.1 Technology Assessment for ICT infrastructure	NA	Does this assessment to be performed across all the 10+ locations highlighted in section 6.2.3?	Yes
4.	Section-III SOW 7.1.3.1 Technology Assessment for ICT infrastructure	1. Discovery of ICT assets and preparation of updated Asset Register	Are there existing asset registers in place? Is the expectation to create the risk register from scratch or update the existing register?	There are no consolidated Asset Register and Risk Register. The bidder shall create these documents from scratch.
5.	Section-III SOW 7.1.3.1 Technology Assessment for ICT infrastructure	2. Review of Endpoint security	How many endpoints are to be covered for each location?	Please refer to Clause 6.1 of SOW, document (1691556855.pdf).
6.	Section-III SOW	3. Review of Network architecture and Network Security	How many network architectures are to be reviewed? Is there only one DC/DR?	Please refer to details mentioned in Clause No. 6.0 CYBERSECURITY CONSTITUENCY of SOW,

	7.1.3.1 Technology Assessment for ICT infrastructure			to estimate. The exact count of network architecture to be reviewed needs to be discovered/assessed during Stage-1 of SOW. OIL has multiple datacenters/server rooms which needs to be discovered/assessed during Stage-1 of SOW.
7.	Section-III SOW 7.1.3.1 Technology Assessment for ICT infrastructure	5. Review of application development practices	What kind of development model is followed? (E.g. - Agile, DevOps) The development is for internal use or for external customers/business? Are the development conducted internally or outsourced to third parties?	OIL follows traditional development model. Developments are conducted both internally and outsourced to third parties.
8.	Section-III SOW 7.1.3.1 Technology Assessment for ICT infrastructure	6. Review of ICT assets on Public Cloud	1) What CSP is currently used for public cloud deployments? Please highlight key services currently used. 2) How many subscriptions/accounts are to be included as part of the scope?	To be discovered/assessed during Stage - 1 of SOW.
9.	Section-III SOW 7.1.3.1 Technology Assessment for ICT infrastructure	8. Active Directory Security Assessment	1) What is the active directory architecture? (E.g. - single tenant, muti tenant) What is the count of the domain controllers present? 2) Approximate number of users and computers in domain 3) On prem AD is integrated with Azure AD?	1) Active directory architecture - Single Tenant. Count of domain Controllers: 2. 2) Please refer to Clause No. 6.1 of SOW, document (1691556855.pdf). 3) Yes, on-prem AD is integrated with Azure AD.
10.	Section-III SOW 7.1.3.1 Technology Assessment for ICT infrastructure	13. Review of Identity and Access Management 14. Review of Privilege Identity and Access Management	What solutions are currently in use for IAM and PAM?	OIL does not have existing IAM and PAM solutions.
11.	Section-III SOW 7.1.3.1 Technology Assessment for ICT infrastructure	19. Review Backup and Recovery practices	What solutions are currently in use for backup and recovery processes?	OIL's backup and recovery processes are distributed and need to be discovered during Stage -1 of SOW.

12.	Section-III SOW 7.1.3.1 Technology Assessment for ICT infrastructure	21. Review of Database security	What type of databases are currently in use? Count of the number of databases servers which are to be included as part of the scope?	OIL has multiple databases which needs to be discovered/assessed during Stage - I of SOW as per the terms and conditions of the tender.
13.	Section-III SOW 7.1.3.1 Technology Assessment for ICT infrastructure	23. Review of Log management and event data collection practices for monitoring and detection of potential cyber threats	What SIEM and SOAR solutions are currently implemented?	This information shall be shared post award of the contract to the successful bidder.
14.	Section-III SOW 7.1.3.2 Technology Assessment for OT infrastructure	1. Discovery of OT assets and preparation of updated Asset Register	Are there existing asset registers in place? Is the expectation to create the risk register from scratch or update the existing register? Is there an existing tool for passive discovery or does the bidder need to use their tools for passive discovery?	There are no consolidated Asset Register and Risk Register. The bidder shall create these documents from scratch. Please be guided by point no. 7 of Clause No. 7.1.2 Methodology of SOW, document (1691556855.pdf).
15.	Section-III SOW 7.1.3.2 Technology Assessment for OT infrastructure	3. Review of Network architecture and Network Security	How many network architectures are to be reviewed? Is the architecture of only refineries or the individual pipelines to be reviewed as well? Do we need to create separate reference diagrams for each entity?	Please refer to details mentioned in Clause No. 6.0 CYBERSECURITY CONSTITUENCY of SOW, document (1691556855.pdf), to estimate. Regarding creation of separate reference diagram for each entity, please be guided by point no. 7.1.4 Deliverables of SOW, document (1691556855.pdf).
16.	Section-III SOW 7.1.3.2 Technology Assessment for OT infrastructure	10. Review of Privilege and Identity Access Management	What solutions are currently in use for PAM in OT environment?	OIL does not have existing PAM solutions.
17.	Section-III SOW 7.1.3.2 Technology Assessment for OT infrastructure	15. Configuration review of OT systems, operations, and controls	What components are to be reviewed as part of this scope? Please specify approximate count of individual components which are to be reviewed. HMI - PLC DCS Windows Server SCADA	Please refer to the point no. 6.6 OT Assets of SOW, document (1691556855.pdf). The OT components needs to be discovered/assessed during Stage - 1 of SOW.

			ESD SIS	
18.	Section-III SOW 7.1.3.2 Technology Assessment for OT infrastructure	23. Review of Log management and event data collection practices for monitoring and detection of potential cyber threats	What solutions are currently implemented in OT for logging and monitoring?	This information shall be shared post award of the contract to the successful bidder.
19.	Section-III SOW 7.1.3.3 Vulnerability assessment (VA), Penetration testing (PT) and application security assessment for both ICT and OT infrastructure	External and Internal VA&PT exercises involving Reconnaissance, Scanning, Vulnerability Analysis, non-destructive Exploitation and Post-Exploitation analysis	What is the approximate count of IP addresses which are to be looked at for the Internal and External VA&PT scope?	Corrigendum shall be published shortly in this regard.
20.	Section-III SOW 7.1.3.3 Vulnerability assessment (VA), Penetration testing (PT) and application security assessment for both ICT and OT infrastructure	External and Internal VA&PT exercises involving Reconnaissance, Scanning, Vulnerability Analysis, non-destructive Exploitation and Post-Exploitation analysis	Will VPN access be provisioned for the internal VA&PT assessment?	Please refer to point no. 2 of Clause No. 7.1.2 Methodology of SOW, document (1691556855.pdf).
21.	Section-III SOW Acceptable Industry Certificates	Pool-3 1. ISA/IEC 62443 Cybersecurity Expert (ICE) 2. GIAC Industrial Cybersecurity Certification (GICSP) 3. Certified SCADA Security Architect (CSSA) 4. Global Industrial Cybersecurity Professional (GICSP)	Is the ISA 62443 Cybersecurity Fundamentals Specialist (IC32) ok instead of ICE?	Corrigendum shall be published shortly in this regard.
22.	Section-III SOW 7.1.3.4 Cybersecurity Governance assessment	Evaluation of incident response and management practices	Do we need to only review the process in line with NCIIPC, CCMP and CERT-IN guidelines or help update the incident response aspects as well?	Please refer to Clause No. 4.0 REFERENCE STANDARDS AND FRAMEWORKS & 5.0 COMPLIANCE TO LEGAL AND GOVERNMENT GUIDELINES of SOW, document (1691556855.pdf) and be guided by the terms and conditions of this tender.
23.	Section-III SOW	The Consultant shall have to design the	Please advise if Oil India shall be going ahead for	Cannot be disclosed.

	4.0 REFERENCE STANDARDS AND FRAMEWORKS	cybersecurity program for OIL in compliance with the following global standards and frameworks:	external certifications for these standards also.	
24.	Section-III SOW 7.1.3.5 Cybersecurity Risk Assessment	The cybersecurity risk assessment exercise shall be used to identify, assess, and prioritize the risks that OIL faces from various cybersecurity threats.	Does Oil India have a risk register in place.	There are no consolidated Asset Register and Risk Register. The bidder shall create these documents from scratch.
25.	Section-III SOW 7.2.3.2 Formulation of Policies, Processes and Procedures	Development of organizational information security policies covering at-least the following areas for both ICT and OT systems	Does Oil India have ISMS policy in place for IT and OT systems	Centralised ISMS policy is not present in OIL.
26.	Number of Consultants	Number of Consultants	Basis the scope of work and timelines mentioned in the RFP, we foresee that the number of resources stipulated to be deployed as per the team structure might be insufficient. Please advise if the team structure can be increased.	The Consultant is permitted to deploy additional manpower as per their requirement.
27.	-	-	We note that there is no express limitation on our liability under the RFP. In accordance with standard industry practice, our aggregate liability under RFP in connection with the services shall be for direct damages and shall be limited to one time the fees paid to us	Please be guided by Clause No. 16.0 LIMITATION OF LIABILITY, point no. b) of Section-I GCC of STC, document 1691556860.pdf.
28.	-	-	We hereby apprise Oil India that the services hereunder, are not intended to be an audit, certification, examination, attestation, special report or agreed-upon procedures.	No comment
29.	-	-	We shall be allowed to retain sufficient documentation as part of our professional records to support and evidence the work performed by it. Such retention shall be	Please be guided by NDA clauses of the NDA published along with the tender.

			subject to obligations of confidentiality mentioned herein.	
30.	Section-III SOW 7.1.3.2	Technology Assessment for OT infrastructure	A. For OT assessments how many total no. of physical locations are there with distinct network and at which locations. B. Based on the maturity of OT infrastructure at OIL, what is the preferred methods to discover OT assets: Tool based, Manual or Hybrid approach. C. For Configuration review and VAPT of OT system, OEM permission will be required to run custom scripts/tools. OIL should coordinate with OEM to get us necessary permissions.	A. Please refer to Clause No. 6.6 OT Assets of SOW, document (1691556855.pdf). The sought details are to be discovered during the Stage - 1 of the SOW, by the Contractor. B. OIL has not specified any specific method to discover OT assets. The methods should be decided by the bidder meeting all the requirements of this tender and adhering to all the terms and conditions of this tender. C. Please be guided by Clauses under 7.1.3.3 Vulnerability assessment (VA), Penetration testing (PT) and application security assessment for both ICT and OT infrastructure of the SOW, document (1691556855.pdf).
31.	Section-III SOW 7.1.3.1.1	Discovery of ICT assets and preparation of updated Asset Register with inventory	A. Is there an existing asset (h/w, s/w, applications, licenses, etc.) management tool/solution in place? B. What is the asset life cycle management process - is it centralized or distributed (location wise/department wise) C. Does the asset discovery scan is in this project scope? D. The asset discovery tool and its licenses are part of the scope? E. Please elaborate - what are the external systems? F. No. of suppliers and third-party vendors? Does it require the TPRM process?	A. OIL does not have a central/consolidated asset discovery/management tool. B. Asset life cycle management is distributed in OIL. C. Yes D. Please refer to point no. 7 of Clause No. **7.1.2 Methodology** and point no. C of Clause No. **8.0 Special Terms** of the SOW, document (1691556855.pdf). Also, be guided by point no. 5 of Clause No. **11.0 Responsibilities of the Contractor** of Section-II SCC of STC, document

				1691556860.pdf. E. Please refer to NIST for "external information system". F. The count as asked here needs to be discovered during the Stage - 1 of the SOW. TPRM process at OIL is required to be assessed as per the terms and conditions mentioned in this tender.
32.	Section-III SOW 7.1.3.1.2	Review of Endpoint security with emphasis on	A. No of end point devices (laptop/desktop) in scope? B. Does servers/VMs are also in scope? if yes, share the details (on-prem/cloud) C. For the patch management - does it required to review the existing patch management process? D. Do we need to assess the existing tool being used for the EP management?	A. To be discovered during the Stage -1 of the SOW. B. Yes. To be discovered during the Stage - 1 of the SOW. C. Yes D. Please be guided by the SOW in this tender.
33.	Section-III SOW 7.1.3.1.3	Review of Network architecture and Network Security with emphasis	A. Does it required to cover all the locations mentioned in the RFP? B. Does the cloud architecture/network infrastructure in scope? C. Does DC & DR network in scope? D. Do we need to perform Red Teaming activity? (black box testing) for the publicly available resources? E. what are the types firewalls (IDS/IPS, NG, WAF, etc.) F. Does Network attached storage and network connected printers in scope? If yes, please share the count?	A. Yes B. Yes C. Yes D. Yes E. To be discovered during the Stage - 1 of the SOW. F. Yes. To be discovered during the Stage - 1 of the SOW.
34.	Section-III SOW 7.1.3.1.4	Review of Software patch management processes and status	List of software in the scope?	The ask is to review the Software patch management processes irrespective of the software in use.

35.	Section-III SOW 7.1.3.1.5	Review of application development practices (application code review is outside the scope of the project)	A. Does application functionality assessment in scope? B. Application testing and Database security are not part of the scope	A. No B. Please be guided by detailed clauses mentioned in the SOW, document (1691556855.pdf).
36.	Section-III SOW 7.1.3.1.6	Review of ICT assets on Public Cloud with emphasis on	A. It will be generic level assessment not the enterprise's level for cloud (the generic level shall cover - authorization, access management, data security (at transection & at rest), data backup, data archival, data restoration, SLA & CIA (confidentiality, Integrity & availability) of services/platform B. The utilization and commercials review/assessment are not part of the scope	A. Please adhere to all the terms, conditions, and asks as mentioned in the tender. B. Please be guided by all the review/assessment mentioned in the SOW, document (1691556855.pdf).
37.	Section-III SOW 7.1.3.1.8	Active Directory Security Assessment (ADSA)	A. How many domains would be there as a part of the scope? B. Is it an on-prem active directory or a Azure/cloud active directory? C. Review operating system configuration, security patch, and update levels - review will be limited the OS (operating System) of AD (Active Directive)	A. 01 (One) B. On prem Active directory C. Please be guided by all the review/assessment mentioned in the SOW, document (1691556855.pdf).
38.	Section-III SOW 7.1.3.1.9	Review of installed security solutions and controls	How many locations need to be covered for physical security?	Please refer to Clause No. 6.0 CYBERSECUIRTY CONSTITUENCY of SOW, document (1691556855.pdf). The installed security solutions and controls need to be discovered/assessed during Stage - 1 of SOW, by the Contractor.
39.	Section-III SOW 7.1.3.1.22	Discovery of shadow IT - the unauthorized use of any digital service or device that is not formally approved of and supported by the IT department.	Need more clarity on Shadow IT activity as the assessment will be on the sampling bases (e.g. asset register vs actual assets, software/license register vs in use)	The assessment shall be based as per the Clause No. 7.1.2 Methodology in SOW document (1691556855.pdf).

40.	Section-III SOW 7.1.3.1.24	Supply Chain and vendor services review	A. Do we need to perform TPRM (third party risk assessment/management)? B. Count of vendors and their priority for TPRM? D. The TPRM assessment will be limited to the ICT & OT vendors.	A. Yes B. To be discovered/assessed during Stage - 1 of SOW, by the Contractor. C. Yes
41.	Section-III SOW 7.1.3.1.25	Identification of critical ICT services for continuity of business operations of OIL	A. Do we need to perform BIA (Business Impact Analyses)? B. Is there a list available identified for the business-critical process/environment (application/services)? C. No. of application/services and or infrastructure/environment to be cover in BIA? D. The BIA process will be limited to the IT & OT environment.	A. Please refer to Clause No. 7.1.3.5 Cybersecurity Risk Assessment in SOW document (1691556855.pdf). B. To be discovered/assessed during Stage - 1 of SOW, by the Contractor. C. Please refer to Clause No. 7.1.3.5 Cybersecurity Risk Assessment in SOW document (1691556855.pdf). D. Yes.
42.	Section-III SOW 7.1.3.3	Vulnerability assessment (VA), Penetration testing (PT) and application security assessment for both ICT and OT infrastructure	A. Do we need to perform a full-fledged red teaming activity covering point 1 & 2? B. Are revalidations (limited to the observation identified during the activity) included as part of scope? C. For mobile applications, what is the OS for these devices (iOS, android or both). D. For OT infrastructure Penetration Testing is not advisable in production environment. OIL to confirm, if they want to conduct PT for OT in production environment, or they have any test laboratory.	A. Please adhere to the requirement/asks mentioned in the SOW of this tender. B. No C. Both android and iOS D. Please refer to point no. 4 of Clause No. 7.1.3.3 Vulnerability assessment (VA), Penetration testing (PT) and application security assessment for both ICT and OT infrastructure of SOW, document (1691556855.pdf)
43.	Section-III SOW 7.1.3.5	Cybersecurity Risk Assessment	A. Does it required to prepare the Risk Register and managed with all the identified gaps during the assessment. B. The risk mitigation plan is to limited to the gaps has been identified	A. Yes B. Yes C. Please be guided by Clause No. 7.3 Stage 3: Development of action plan of the SOW,

			during the assessment activity. C. Recommendations for mitigation is limited to the road map activity where we will share the project plan considering how OIL can reduce the risk - the implementation of the mitigation plan is out of the scope.	document (1691556855.pdf)
44.	Section-III SOW 7.2.3.3	Development of Target State Architecture for Technology Infrastructure	The design and development of the architecture will be limited to the HLD (High level design document)	The details of the target state architecture as required in the SOW should be provided by the Contractor.
45.	Section-III SOW 7.3.3.1.1	Development of the Action Plan	OFI prioritization shall be limited to the gaps identified during the assessment as per the scope.	Yes
46.	Section-III SOW 7.3.3.1.3	Further clarification of the OFIs into the following two categories:	The suggestions shall be limited to the gaps identified during the assessment (as per the scope) and the implementation is not part of the scope.	Please be guided by the terms and conditions of the SOW, document (1691556855.pdf)
47.	Section-III SOW 7.3.3.2.1	Development of Action Plan	Does it require to perform the Maturity Assessment?	Yes, it is part of STAGE - 1: AS-IS ASSESSMENT in the SOW.
48.	Section-III SOW 7.3.3.2.2	Amongst the prioritized OFIs, OIL shall select 10 (Ten) tactical and 05 (Five) strategic OFI for immediate action.	Decision for Prioritization and selection of immediate action out of the suggested action plan shall be responsibility of OIL.	Yes.
49.	Section-III SOW 7.4.3.1	Workshop and Presentation to the Management	A. How many workshops need to be conducted for top management & functional head? B. the workshop shall be limited to cover the findings and the remediation plan.	Please be guided by Clause No. 7.4.3 List of Activities of the SOW, document (1691556855.pdf)
50.	Section-III SOW 7.4.3.2	Awareness training to the Core Team Members	A. How many workshops need to be conducted for core members? B. the workshop will be limited to cover the findings and the remediation plan.	Please be guided by Clause No. 7.4.3.2 Awareness Training to Core Team members of the SOW, document (1691556855.pdf)
51.	Section-III SOW 6.8	Web & Mobile Application Total number of Applications - 40	Kindly confirm the count.	Please be guided by the information mentioned in SOW, document (1691556855.pdf)

		Total No. of Mobile applications - 10		
52.	Section-III SOW 6.5	Network Internal Firewalls - 6 Firewalls - 22 Routers - 50 Switches - 250	Please confirm the count. Also kindly provide Network/wifi access point count?	Please be guided by the information mentioned in SOW, document (1691556855.pdf)
53.	Section-III SOW 7.1.5	Stage - 1: As-Is Assessment (It is required on site during the entire stage-1 activity)	A. Is it possible to manage the stage-1 activity in hybrid mode? The resources will visit the sites on need basis alignment with the relevant stakeholders based on the project requirements? B. The stage-1 activity requires to travel all the office locations of IT assessment and relevant plants/sits for OT - Do we get the guesthouse and local transport facilities at all the locations mentioned in the RFP?	Please be guided by point no. 2 of Clause No. 7.1.2 Methodology of the SOW (1691556855.pdf) and point no. 6 of Clause No. 11.0 Responsibilities of the Contractor of the STC, document 1691556860.pdf
54.	Section-III SOW 7.2.5	Stage-2: Development of the Cybersecurity Program (Minimum 5 days on site)	Do we get the guesthouse and local transport facilities?	Please refer to point no. 6 of Clause No. 11.0 Responsibilities of the Contractor of Section-II SCC of the STC, document 1691556860.pdf
55.	Section-III SOW 7.3.5	Stage-3: Development of Action Plan (Minimum 10 days on site)		
56.	Section-III SOW 7.4.5	Stage - 4: Communication to Stakeholders and Project Closure (Minimum 2 days on site (one location for 2 days)		
57.			Request OIL to increase the project duration to 12 months. Also, request OIL to allow bidders to manage individual milestone schedule as per the project requirements.	Corrigendum shall be published shortly in this regard.
58.	PQC/BEC/BRC QCBS	The bidder shall submit the Curriculum Vitae (CV) of the proposed personnel as per Annexure-II along with their offer. The CV shall be enclosed with following documentary proof: • Identity Proof	PwC will submit the CVs of the resources during bidding process. Documentary proof shall be furnished after award of contract, if required.	Not acceptable.

		• Date of Birth Proof • Proof of educational qualification • Proof of Experience		
59.	PQC/BEC/BRC Notes to BEC Clause 3.0 above: Point No. B	The bidder shall provide valid certificates from CERT-IN in their offer confirming that the bidder is currently empanelled by CERT-In as Information Security Auditing Organization, along with an undertaking to maintain its validity throughout the contract period.	Is there a specific format for the undertaking for certificate renewal?	There is no specific format for the undertaking. It may be submitted in bidder's Company letter head duly signed by the authorised signatory of the Company.
60.	PQC/BEC/BRC Notes to BEC Clause 3.0 above: Point No. C	The bidder shall provide valid certificates from ISO/IEC conforming that the bidder is ISO/IEC 27001:2013 or ISO/IEC 27001:2022 certified, along with an undertaking to maintain its validity throughout the contract period.	Is there a specific format for the undertaking for certificate renewal?	There is no specific format for the undertaking. It may be submitted in bidder's Company letter head duly signed by the authorised signatory of the Company.
61.	PQC/BEC/BRC Clause No. 4 B)	2 Nos. Subject Matter Expert – ICT Security i) Qualification: BE/BTech with at least any three of the certificates from Pool-2 (Clause No. 3.1.2 I) of SOW)	Please clarify what will be the combination of Resource and CVs to score maximum marks against this category.	This is bidder's responsibility.
62.	PQC/BEC/BRC Clause No. 4 B)	02 Nos. Subject Matter Expert – OT/ICS Security i) Qualification: BE/BTech with at least any two of the certificates from Pool-3 (Clause No. 3.1.2 I) of SOW)	1.Please clarify what will be the combination of Resource and CVs to score maximum marks against this category.	This is bidder's responsibility.
63.	PQC/BEC/BRC QCBS, Clause no. 5 (3.2.4)	3.2.4.3 Certificate from Pool-3 a) 05 or more distinct certificates from Pool-3	1) Kindly elaborate regarding the requirement for distinct certificates. 5 distinct certificates from Pool 3 - Should we produce 5 resources with any of the certificates from pool or we need to have 5 distinct	1) Corrigendum shall be published shortly in this regard. 2) Please refer to point-5 of notes of Clause No. 5.0 QUALITY & COST BASED SELECTION (QCBS)-SCORING AND

			certificates with the available resources. 2) To achieve maximum rating of the certificate criteria, we will share maximum count based on the eligibility. Do we need to deploy all those resources, or we can select the resources for project deployment among the CVs we have submitted during the bid to cover the project requirements (1 PM, 2 ICT SME, 2 OT SME, 1 CS Governance, 1 QA and 2 QR)	EVALUATION CRITERIA in PQC document 1691571229.pdf.
64.	Section-III SOW Clause No. 3.1.2 Acceptable Industry certificate	Pool 3 1. ISA/IEC 62443 Cybersecurity Expert (ICE) 2. GIAC Industrial Cybersecurity Certification (GICSP) 3. Certified SCADA Security Architect (CSSA) 4. Global Industrial Cybersecurity Professional (GICSP)	1. We request OIL to include IEC 62443 fundamental specialist certificate in Pool3.	Corrigendum shall be published shortly in this regard.
65.	PQC/BEC/BRC Clause No. 3.1	Cybersecurity consultancy services for assessment of cybersecurity risk and development of cybersecurity program for ICT (Information and Communications Technology) systems, under single contract. AND Cybersecurity consultancy services for assessment of cybersecurity risk and development of cybersecurity program for OT (Operational Technology) systems, under single contract.	Different clients use different terminologies in their POs. Request you to consider cyber security risk assessment and gap analysis/cyber security advisory services/recommendations/cyber security program development as relevant experience.	Corrigendum shall be published shortly in this regard.
66.	PQC/BEC/BRC Clause No. 3.1	Cybersecurity consultancy services for assessment of cybersecurity risk and development of cybersecurity program	1) Kindly confirm whether the experience is considered in India or globally?	Corrigendum shall be published shortly in this regard.

		for ICT (Information and Communications Technology) systems, under single contract. AND Cybersecurity consultancy services for assessment of cybersecurity risk and development of cybersecurity program for OT (Operational Technology) systems, under single contract.		
67.	PQC/BEC/BRC QCBS, Clause Nos. 5.1 and 5.2	Experience in providing 'cybersecurity consultancy services for assessment of cybersecurity risk and development of cybersecurity program for ICT (Information and Communications Technology) systems' during the last 07 (Seven) years reckoned from the original bid closing date. Experience in providing 'cybersecurity consultancy services for assessment of cybersecurity risk and development of cybersecurity program for OT (Operational Technology) systems' during the last 07 (Seven) years reckoned from the original bid closing date.	1) Kindly confirm whether the experience is considered in India or globally? 2) Kindly clarify if any minimum value criteria of work order is asked?	1) Corrigendum shall be published shortly in this regard. 2) Corrigendum shall be published shortly in this regard.
68.	Proforma-II of Tender	No deviation but RFP has a format for statement of non-compliance (only exceptions/deviations to be rendered)	Kindly clarify whether submission of statement of non-compliance submission will lead to automatic disqualification from tendering process	The bidder is requested not to submit any exception/deviation. If bidder has any queries related to tender, it is requested to get clarified prior to the bid closing date.
69.	STC Section-I GCC, Clause No. 16 (b) (Limitation of Liability)	There are following exceptions to the limitation of liability - cost of repairing or	OIL is requested to delete exceptions to the limitation of liability. The exceptions render the limitation of liability	These are the standard clauses of the General Conditions of Contract (GCC). There shall be no change in the clause.

		replacing defective equipment by the CONTRACTOR, or to any obligation of the CONTRACTOR to indemnify the COMPANY with respect to Intellectual Property Rights.	ineffective and make the liability unlimited.	
70.	Art. 8 pf NDA doc. (Confidentiality Obligations)	Obligations to survive is perpetual	We request OIL to reduce the survival period of confidentiality obligations to one year post expiry or termination.	Not acceptable. No change in the clause.
71.	STC Section-I GCC, Clause No. 26.3 (Confidentiality Obligations)	Obligation to return all confidential information/destroy all confidential and no right to retain a copy	We request OIL to allow us to retain our working papers and a copy of confidential information for our records and any future reference or audit requirements, subject to confidentiality obligations under this Agreement.	These are the standard clauses of the General Conditions of Contract (GCC). There shall be no change in the clause.
72.	STC Section-I GCC, Clause No. 16(b), Section-I GCC, Clause No. 22 (Indemnity)	Indemnities for IPR infringement claims without exceptions	We request OIL to include the following exceptions and procedure as these are industry standards and reasonable. They are also mentioned in the MeitY guidelines. *"1. Notwithstanding anything contained in this agreement, if the Indemnified Party promptly notifies Indemnifying Party in writing of a third party claim against Indemnified Party that any Service provided by the Indemnifying Party infringes a copyright, trade secret or patents incorporated in India of any third party, Indemnifying Party will defend such claim at its expense and will pay any costs or damages, that may be finally awarded against Indemnified Party. 2. Indemnifying Party will not indemnify the Indemnified Party, however, if the claim of infringement is caused by:*	These are the standard clauses of the General Conditions of Contract (GCC). There shall be no change in the clause.

			a) Indemnified Party's misuse or modification of the Service; b) Indemnified Party's failure to use corrections or enhancements made available by the Indemnifying Party; c) Indemnified Party's use of the Service in combination with any product or information not owned or developed by Indemnifying Party; However, if any service, information, direction, specification or materials provided by Indemnified Party or any third party contracted to it, is or likely to be held to be infringing, Indemnifying Party shall at its expense and option either: i. Procure the right for Indemnified Party to continue using it; ii. Replace it with a non-infringing equivalent; iii. Modify it to make it non-infringing. *3. The foregoing remedies constitute Indemnified Party's sole and exclusive remedies and Indemnifying Party's entire liability with respect to infringement."*	
73.	STC Section-I GCC, Clause No. 15.2, Section-I GCC, Clause No. 20, Section-I GCC, Clause No. 21 at pg. no. 20 (Indemnity)	Indemnity for breach of contract obligations	There are several remedies available under law and contract to you for such breach of obligations. For eg., there are penalties and LDs that may be imposed for some of these breaches. We understand that remedies other than indemnity will be sufficient for such breaches. We request you to kindly delete this section. If you still insist on retaining this section, then we request you to at least make them subject	These are the standard clauses of the General Conditions of Contract (GCC). There shall be no change in the clause.

			to overall cumulative liability cap of total contract value and subject to final determination of court/arbitrator.	
74.	STC Section-I GCC, Clause No. 15.6 (Indemnity)	Indemnities for death and bodily injury	Request OIL to kindly delete these. Alternatively, kindly cap these indemnities to limitation of liability cap or one time the fees payable to us under this Agreement.	These are the standard clauses of the General Conditions of Contract (GCC). There shall be no change in the clause.
75.	No clause in RFP. Please include in pre-bid.	Termination without notice and rectification period	To uphold the principles of natural justice, we request OIL to notify us and give us a rectification period of at least 30 days, prior to invoking this clause.	Not acceptable.
76.	No clause in RFP. Please include in pre-bid.	We do not have any right to terminate	To uphold the principles of natural justice and to bring parity in the contract, we request OIL to give us the right to terminate the contract in case client breaches any of its material obligations under the contract, provided a notice for such breach is given to client along with a rectification period of 30 days.	Not acceptable.
77.	STC, Section-I GCC, Clause No. 19 at (STC)	Risk purchase	Request OIL to limit our liability under this clause to 10% of the value of corresponding goods/services not delivered by us. Please also confirm that client will use government procurement norms (including price discovery) for procurement of such services from third parties.	These are the standard clauses of the General Conditions of Contract (GCC). There shall be no change in the clause.
78.	STC, Section-I GCC, Clause No. 30, Liquidated Damages	LDs capped at more than 7.5%	We request OIL to cap the liquidated damages cumulatively to 5% of the total contract value.	These are the standard clauses of the General Conditions of Contract (GCC). There shall be no change in the clause.
79.	STC, Section-I GCC, Clause No. 30, Liquidated Damages	Not sole and exclusive remedy	We understand that as per Contract Act, where LDs are stipulated, generally any other damages cannot be	These are the standard clauses of the General Conditions of Contract (GCC). There shall be no change in the clause.

			claimed. Therefore, we request you to kindly make imposition of liquidated damages as sole and exclusive remedy for corresponding breaches.	
80.	STC, Section-I GCC, Clause No. 30 Liquidated Damages	Not limited to solely our fault	We understand that we would be liable to pay liquidated damages to the extent corresponding breach is solely attributable to us. Kindly confirm.	Please be guided as per the clauses mentioned under Clause No. 30.0 of Section-I, GCC.
81.	STC, Section-I GCC, Clause No. 30.0	Times is of essence and LDs for delay	By making time of essence of the contract, you retain the right to void the contract ab initio in case timelines are not met. There are various dependencies on the client and other third parties for completing the project. There may be delays on part of client and other parties also. Thus, contract can be voided by you even if the fault is not entirely ours. We understand that it is not the intention to make the agreement void ab initio in case of any delay in achieving the timelines. Further, since there are LDs for delay in achieving the timelines, it does not look legally feasible to have time as essence of the contract. Thus, request you to kindly delete this clause.	These are the standard clauses of the General Conditions of Contract (GCC). There shall be no change in the clause.
82.	No clause in RFP. Please include in pre-bid.	No protection to our pre-existing IPRs	There are innumerable IPRs that exist with us which we would like to use to your benefit while delivering our services to you. These are our pre-existing IPRs and we use it for all clients. We will not be able to give ownership in such IPRs to you just because we are using them for providing services to you, like we use these for	Not acceptable.

			other clients. We request that we are allowed to retain ownership of our pre-existing IPRs, else we might not be able to use these in providing services to you in order to protect our ownership in them. We request you to kindly include the below clause. This is also the standard mentioned by MeitY in its guidelines. *"Notwithstanding anything to the contrary in this agreement, Consultant will retain the ownership of its pre-existing intellectual property rights (including any enhancement or modification thereto) even if such IPRs are used for creating deliverables, are incorporated in the deliverables, etc. To the extent such pre-existing IPRs are included/incorporated in the deliverables, upon receipt of all due and payable payment in full, the Consultant shall grant a non-exclusive, perpetual and fully paid-up license to the Purchaser/Client to use such pre-existing IPRs for use of deliverables for the purpose for which such deliverables are meant for client's internal business operations."*	
83.	STC, Section-I GCC, Clause No. 14.	Insurance - Wide insurance procurement obligations	We wish to clarify that we maintain insurances, at the firm level, which are required to be maintained by us as per the provision of laws. Separate insurances for this project may not be required in light of such firm level insurance. We can provide you with a confirmation about our firm level insurance and that to the extent	Please be guided as per clauses mentioned under Clause No. 14.0 of Section-I GCC.

			required by law, this project will also be covered under that insurance. We hope that should suffice. Please confirm.	
84.	STC, Section-I GCC, Clause No. 25	Inspection - Widely worded rights	We wish to clarify that we will retain our records as per our records retention policies. Upon reasonable notice, we will allow OIL to inspect our invoicing records under this engagement; such inspection shall be done in a pre-agreed manner and during normal business hours. For avoidance of doubt, such inspection should not cause us to be in breach of our organizational confidentiality requirements. Please acknowledge that our audit related obligations will be subject to foregoing statement.	Please be guided as per Clause No. 25.0 of Section-I GCC.
85.	STC, Section-I GCC, Clause No. 42(4)	Arbitration	In order to uphold the principles of natural justice (Nemo judex in causa sua- no one should be judge in one's own case) and the provisions of the Arbitration and Conciliation Act, we request that the arbitrator(s) be appointed with mutual consent of both the parties. Alternatively, a panel of three arbitrators may be set up in which one arbitrator is appointed by consultant, one by the client and the two arbitrators appoint third arbitrator. Please confirm.	Please be guided as per Clause No. 42.0 of Section-I GCC.
86.	No clause in RFP. Please include in pre-bid.	There is no restriction on the usage of deliverable. No third-party disclaimers.	We will be providing services and deliverables to you under the contract. We accept no liability to anyone, other than you, in connection with our services, unless otherwise agreed by us in writing. You agree to	Please be guided as per tender document.

			reimburse us for any liability (including legal costs) that we incur in connection with any claim by anyone else in relation to the services. Please confirm our understanding is correct.	
87.	No clause in RFP. Please include in pre-bid.	No acceptance criteria	If the project is to be completed on time, it would require binding both parties with timelines to fulfil their respective part of obligations. We request you that you incorporate a deliverable acceptance procedure, perhaps the one provided by MeitY in their guidelines, or the one suggested below, to ensure that acceptance of deliverables is not denied or delayed and comments, if any, are received by us well in time. You may consider including the below simple clause: *"Within 10 days (or any other agreed period) from Client's receipt of a draft deliverable, Client will notify Consultant if it is accepted. If it is not accepted, Client will let Consultant know the reasonable grounds for such non acceptance, and Consultant will take reasonable remedial measures so that the draft deliverable materially meets the agreed specifications. If Client does not notify Consultant within the agreed time period or if Client uses the draft deliverable, it will be deemed to be accepted."*	Not acceptable.
88.	PQC/BEC/BRC Clause No. 3.0	i) Cybersecurity consultancy services for assessment of cybersecurity risk and development of cybersecurity program	As stated within PQC, Technical Criteria 3.1 I (i & ii), the current stipulation allows only completed projects. We kindly request the	Please be guided by point no. D of the "Notes to BEC Clause No. 3.0" in PQC, document (1691571229.pdf)

		for ICT (Information and Communications Technology) systems, under single contract. AND ii) Cybersecurity consultancy services for assessment of cybersecurity risk and development of cybersecurity program for OT (Operational Technology) systems, under single contract.	esteemed team to also take ongoing projects into consideration. We would like to request the authority to please consider the above request of ongoing projects.	
89.	Section-III SCOPE OF WORK (SOW)_1691556855 Section-6.5 Network	Network Devices: Internal Firewalls: 6 Firewalls: 22 Routers: 50 Switches: 250	Configuration review for all Router & Switches will be in scope or on sample basis?	Please be guided by point no. 3 of Clause No. 7.1.2 Methodology of the SOW, document (1691556855.pdf).
90.	Section-III SCOPE OF WORK (SOW)_1691556855 Section-6.5 Network	Cloud Assets	Number of CSP accounts where Cloud security assessment to be conducted.	To be discovered/assessed during Stage - 1 of SOW.
91.	Section-III SCOPE OF WORK (SOW)_1691556855 Section-6.5 Network	Web & Mobile Application: 1. Total number of Applications: 40 2. Total No. of Mobile applications: 10	Are all the applications having production/test/dev environment? On which environment, application testing to be conducted? Request you to mention the application testing methods: blackbox/greybox	OIL has different landscape architecture for different applications, which the contractor should identify during the Stage - 1 as per the SOW. Also, please be guided by point no. 4 of Clause No. 7.1.3.3 of the SOW, document (1691556855.pdf). Regarding testing method, please refer to the corrigendum that shall be published shortly.
92.	Section-III SCOPE OF WORK (SOW)_1691556855 Section-7.1.2 Methodology	The team of consultants responsible for carrying out the assessment activities shall visit all the locations of OIL as specified in [6.2] for the assessment exercise. The consultants shall be onsite at OIL's offices for the entire duration of this stage.	For which activities consultants will visit locations. Is OIL will provide expenses/accommodations/conveyance or its to be included in project cost. Are all the ICT Assets (applications, cloud instances and IPs/Devices) are remotely accessible through VPN or at least accessible from OIL Kolkata office to conduct the assessments.	Please refer to the terms and conditions (specially Methodology section of each stage) mentioned in the SOW, document (1691556855.pdf). Also, please be guided by point no. 6 of Clause No. 11.0 Responsibilities of the Contractor of Section-II SCC of the STC, document 1691556860.pdf

93.	Section-III SCOPE OF WORK (SOW)_1691556855 Section-7.1.3.3 Methodology	ICT Infrastructure VAPT	Number of ICT and OT assets/IP to be conducted infrastructure VAPT	Please refer to point no. 6.3 ICT Assets and 6.6 OT Assets of SOW, document (1691556855.pdf). The ICT and OT components need to be discovered/assessed during Stage - 1 of SOW, by the contractor.
94.	Section-III SCOPE OF WORK (SOW)_1691556855 Section-7.1.3.2 Technology Assessment for OT infrastructure	OT Assets	Count of units/plants to be covered as part of assessment along with the sizing of each unit (inventory/systems/ sensors/HMIs/ ES/ OS) is not mentioned in RFP. Please clarify. This is required to the effort estimation	Please refer to Clause No. 6.6 OT Assets of SOW, document (1691556855.pdf). The OT components need to be discovered/assessed during Stage - 1 of SOW, by the contractor.
95.	Section-III SCOPE OF WORK (SOW)_1691556855 Section-7.1.3.3 Technology Assessment for OT infrastructure	OT Infrastructure VAPT	Vulnerability assessment (VA), Penetration testing (PT) and application security assessment for OT is not applicable with OWASP Top 10 risk, request you to mention alternate standard	OWASP is mentioned for web and mobile application VA & PT only, in point no. 3 of Clause No. 7.1.3.3 -Vulnerability assessment (VA), Penetration testing (PT) and application security assessment for both ICT and OT infrastructure of SOW, document (1691556855.pdf)
96.	Section-III SCOPE OF WORK (SOW)_1691556855 Section-7.1.3.5 Cybersecurity Risk Assessment	OT Cybersecurity Risk Assessment	As OT security risk assessment need to be performed. Please confirm if bidder need to limit to High-level risk assessment or Low-level risk assessment?	The assessment should suffice/meet all the terms and conditions/requirements as mentioned in this tender.
97.			Due to the complex Project to deliver, we hereby request you to allow consortium to participate in the said RFP.	Not acceptable
98.			Request you to clarify the duration of projects for each professional	It is bidder's responsibility to determine the duration for each professional adhering to all the terms and conditions mentioned in the tender document.
99.			Please clarify that during the project delivery or during maintenance services, whether we can	Please be guided by point no. 10 of Clause No. 11.0 Responsibilities of the Contractor Section-II of SCC of the STC,

			change professionals or not?	document 1691556860.pdf
100.			Request you to clarify is that the quality assurance different from project manager	Yes. Please refer to point no. 3 of Clause No. 3.1.1 in SOW document, 1691556855.pdf
101.	PQC/BEC/BRC Clause No. 2.0	The bidder must be incorporated/registered in India and must maintain more than or equal to 20% local content (LC) for the offered services to be eligible to bid against this tender.	Clarification required on the specifics of local content as mentioned in the clause.	Please refer Purchase preference under Public Procurement (Preference to Make in India) Order, 2017 of Department for Promotion of Industry and Internal Trade (DPIIT), Govt. of India as revised vide Order No**. P-45021/2/2017-PP (BE-II)** dated **16th September 2020** (and as amended time to time) with modifications as notified vide MoPNG Order No. **FP-20013/2/2017-FP-PNG-Part (4) (E-41432)** dated **26th April 2022.**
102.	PQC/BEC/BRC Clause No. 3.0	3.1 The bidder must be a consultancy firm having experience in providing the followings during the last 07 (Seven) years reckoned from the original bid closing date in Central Govt./State Govt./Public Sector Undertaking/State Govt. Enterprise/Public Limited Company: i) Cybersecurity consultancy services for assessment of cybersecurity risk and development of cybersecurity program for ICT (Information and Communications Technology) systems, under single contract. **AND** ii) Cybersecurity consultancy services for assessment of cybersecurity risk and development of	Request to modify the clause as: i) Cybersecurity consultancy services for assessment of cybersecurity risk and development of cybersecurity program for **IT**/ICT (Information and Communications Technology) systems, under single contract. **AND** ii) Cybersecurity consultancy services for assessment of cybersecurity risk and development of cybersecurity program for OT (Operational Technology) systems, under single contract.	Corrigendum shall be uploaded shortly in this regard.

		cybersecurity program for OT (Operational Technology) systems, under single contract.		
103.	PQC/BEC/BRC Notes to BEC Clause 3.0 above: Point No. A)	A) In support of the experience mentioned above (Clause No. 3.1), the Service Provider/Bidder must furnish the details of the Contracts executed by them in tabular form in ANNEXURE-I along with self-attested photocopies of the following documentary evidence(s): (i) Contract(s) [Relevant pages of the Contract(s) executed]/Work-order(s)/service order(s)/Letter of Award(s)/Letter of Intent(s) indicating Scope of service(s), work, contract period. **AND** (ii) Completion certificate(s)/Final Payment certificate(s) issued by the client(s) for each of the above Contracts or any other document(s), which can substantiate the successful execution of work.	Request to modify the clause as: (i) Contract(s) [Relevant pages of the Contract(s) executed]/Work-order(s)/service order(s)/Letter of Award(s)/Letter of Intent(s) indicating Scope of service(s), work, contract period. AND (ii) Completion certificate(s)/Final Payment certificate(s) issued by the client(s) for each of the above Contracts or **CA Certificate by the Bidder for receipt of payemnt** or any other document(s), which can substantiate the successful execution of work.	No change. Already covered in the existing clause by "any other document(s)".
104.	PQC/BEC/BRC Clause No. 4.0, Core team Experience	As a part of the project execution, bidder shall deploy the followings: A) A Consultant's Steering Committee Member.	(1) Clarification required on the role and requirement of the Consultant's Steering Committee member. (2) Request for the elimination of the requirement.	1) Please refer to point 1 of Clause No. 3.1.1 Structure of the SOW, document (1691556855.pdf). 2) Not acceptable
105.	PQC/BEC/BRC QCBS Clause No. 3.2.4	3.2.4 Industry Certificate 15 (max) Team members (excluding the Project Manager) with acceptable industry certificates.	Request to eliminate the clause. The alignment of number of certifications of team members from each mentioned pool may not be a feasible along with experience.	Not acceptable
106.	Section-III SOW Clause No. 3.1.2	3.1.2 Human Resources IV) Quality Assurance Team	We understand that QA team does not require to be deployed onsite, and it is Bidder's internal	The Consultant shall constitute a team independent from the Project Delivery Team for

		The Consultant shall deploy a Quality Assurance Team for quality review of the project deliverables.	responsibility to ensure quality of deliverables. Please confirm whether our understanding is correct.	quality assurance (QA) of the project deliverables. This team shall be responsible for quality review of the project deliverables before delivery to OIL. Also please refer to the corrigendum (to be published) regarding the QA team's onsite deployment.
107.	STC, Section-II (SCC) Clause No. 9.0	Contract Period/6 Month(s)	The scope of work outlines very comprehensive and detailed activities to be performed by selected bidder. To complete all the deliverables successfully, six months is not adequate timeline considering various dependencies and requirement of scope. We request modification to the clause as **completion time - one year**. No. of deliverables - 134	Corrigendum shall be uploaded shortly in this regard.
108.		No timeline Stage wise mentioned in the RFP.	It is understood that the timelines for respective Stages of Scope of work may vary and does not have a fixed timeline. Request to confirm our understanding.	Corrigendum shall be uploaded shortly in this regard.
109.	PQC/BEC/BRC Clause No. 5.0 QCBS Note No. 2 under Clause No. 3. Of the table	To substantiate this, the bidder must submit CVs including copies of the industry certificates and qualifications of the proposed team members, certified by the CEO/Country Head/Chief Operating Officer or a partner with Power of Attorney, along with the bid.	Request to modify the clause as: "the bidder must submit CVs including copies of the industry certificates and qualifications of the proposed team members, **certified by the CEO/Country Head/Chief Operating Officer or a partner with Power of Attorney or an HR certificate, along with the bid**"	Corrigendum shall be uploaded shortly in this regard.
110.	PQC/BEC/BRC QCBS	The weightage for quality is 60 and the weightage for the quoted price is 40 i.e., Quality: Quoted Price is 60:40.	Considering the organization strong expectations, highly competitive technical evaluation parameters, it is requested to modify the **QCBS evaluation ratio**	Shall be reviewed

			to 80:20. The 60:40 ratio of QCBS tends to L1 bidders.	
111.	Section-III SOW Clause No. 1.0	Identifying and analysing cybersecurity risks, redesigning systems for mitigation	Could you please remove this point from SOW, as the mitigation of identified risk will be out of the scope	"Redesigning systems for mitigation" is part of the scope, however actual implementation shall be out of the scope. Corrigendum shall be uploaded shortly in this regard.
112.	Section-III SOW Clause No. 3.1.2 Project delivery team	Relevant documents confirming to the above must be submitted along with the technical bid.	Could you please confirm what are the expected supporting documents	Please be guided by point no. 4.0 CORE TEAM EXPERIENCE and point no. 2 of the Note in 3.2.4 - Industry Certificate of the QCBS, of the PQC, document 1691571229.pdf
113.	Section-III SOW 7.1.3.2 Technology Assessment for OT infrastructure	Discovery of OT assets and preparation of updated Asset Register	Could you please confirm if there are any existing asset discovery tool that are already present at IOL network	OIL does not have a central/consolidated asset discovery tool.
114.	Section-III SOW 7.1.3.2 Point No. 3	Review of installed security solutions and controls	Could you please clarity the number of security solutions that are in scope	Please refer to point no. 6.0 CYBERSECUIRTY CONSTITUENCY of SOW, document (1691556855.pdf). The installed security solutions and controls need to be discovered/assessed during Stage -1 of SOW, by the contractor.
115.	Section-III SOW 7.1.3.2 Point No. 6	Review controls related to Data security	Could you please elaborate the requirement of Data security controls pertaining to OT	Please refer to 4.0 REFERENCE STANDARDS AND FRAMEWORKS 5.0 COMPLIANCE TO LEGAL AND GOVERNMENT GUIDELINES of SOW, document (1691556855.pdf). and be guided by relevant controls prescribed in the standards and frameworks.
116.	Section-III SOW 7.1.3.2 Point No. 17	Supply Chain and vendor services review	Could you please clarity the exact requirement. Are we expected to perform the third-party risk assessment OT or the scope is limited to the process review	Please refer to Clause No. 4.0 REFERENCE STANDARDS AND FRAMEWORKS & 5.0 COMPLIANCE TO LEGAL AND GOVERNMENT GUIDELINES of SOW, document

				(1691556855.pdf) and be guided by relevant controls prescribed in the standards and frameworks.
117.	Section-III SOW 7.1.3.3 Point No. 2	Both External and Internal VA&PT exercises	could you please clarity what kind of VA & PT testing exercise are expected to be performed on OT systems	Corrigendum shall be uploaded shortly in this regard.

Notes:

i) All bidders were advised to send their additional queries (if any) by 16.09.2023. Any queries received beyond 16.09.2023 shall not be entertained.

ii) Please be informed that the GCC of the tender are standard approved Clauses, therefore deviation to these Clauses is not possible. However, the Clauses of SCC shall supplement and/or amend the GCC. Whenever there is a conflict, the provisions in SCC shall prevail over those in the GCC.