

SOLAR ENERGY CORPORATION OF INDIA LIMITED
NEW DELHI

Ref No. SECI/C&P/EOI/17/0004/26-27/Amendment-01

Date: 05.10.2026

Amendment-01 to Request for Empanelment of CERT-In empaneled Auditors for RE Sector			
Tender No. SECI/C&P/EOI/17/0004/26-27 dated 28.08.2026			
S. No.	Clause No.	Existing Clause	Amended Clause
1.	General	1. Any reference to the “CEA Regulations” in the RfE document and in any documents/communication during the empanelment period shall mean reference to the Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2026 , as amended from time to time.	
2.	1.2	 Given that the CEA Cyber Security Regulations 2024 mandate periodic cybersecurity audits for RE power plants, it is essential for SECI to meaningfully discharge its CERT-RE mandate,...	 Given that the Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2026 mandate periodic cybersecurity audits for RE power plants with an aggregate installed capacity of 50 MW or more, it is essential for SECI to meaningfully discharge its CERT-RE mandate,...
3.	3.1	these empaneled Auditors will be responsible for evaluating, verifying, and enhancing the cybersecurity posture of renewable energy power plants across India,....	these empanelled Auditors will be responsible for evaluating, verifying, reporting and recommending improvements in the cybersecurity posture of renewable energy power plants across India,....
4.	3.3.i.	Purpose: Performed prior to the initialization and grid-synchronization of the renewable energy plant to ensure that baseline security controls are fully established.	Purpose: Performed prior to the initialization and grid-synchronization of the renewable energy plant.
5.	3.3.ii.	Initial Plant Deadline: The first periodic audit must be successfully closed within one year from the exact date of plant commissioning	Deleted.
6.	3.4	The audit methodology and deliverables shall conform strictly to the NIST Cybersecurity Framework (CSF), IEC 62443, ISO/IEC 27001 , and all applicable guidelines, advisories, and regulations issued by the Government of India, Ministry of New and Renewable Energy (MNRE), Ministry of Power (MoP), CEA, and CERT-In from time to time.	The audit methodology and deliverables shall conform strictly to the NIST Cybersecurity Framework (CSF), IEC 62443, ISO/IEC 27001 , and all applicable guidelines, advisories, and regulations issued by the Government of India, Ministry of New and Renewable Energy (MNRE), Ministry of Power (MoP), CEA, and CERT-In from time to time. Annexure B of the RfE will be suitably modified by SECI from time to time, to incorporate any update in

			standards/guidelines as mentioned above.
7.	3.5	Auditors must review, physically verify, and sign off on documentation and deployment architectures across the Audit Parameters mentioned in Annexure-B .	Auditors shall review, verify, and sign off on documentation and deployment architectures across the Audit Parameters mentioned in Annexure-B .
8.	4	Clause revised as per Annexure-I	
9.	5.1.iv.	Zone 4 (Eastern): Bihar, Jharkhand, Odisha, West Bengal, Sikkim, Northeastern States	Zone 4 (Eastern): Bihar, Jharkhand, Odisha, West Bengal, Sikkim, Assam, Arunachal Pradesh, Manipur, Nagaland, Mizoram, Meghalaya, Tripura The table in Covering Letter (Format 7.1) stands suitably modified based on above.
10.	6.1	Clause modified as follows: Initiation and Requisition - In line with the applicable mandates as per the CEA Regulations, 2026, the RE Plants having aggregate installed capacity of 50 MW and above, shall be required to conduct periodic audit of the assets. To facilitate and expedite this, SECI will keep a registry of such eligible plants, with timely notifying such Project Developers to carry out the audits. It is however, clarified that the responsibility of compliance with the applicable Regulations, and therefore, deciding to conduct audits of the plant assets, shall be solely at the risk and cost of the respective Plant Developer. - The Plant Developer will intimate SECI about its interest in conducting the plant's audit through an Auditor empanelled by SECI, which will be known as "Requisition by the Developer." - The above requisition shall be formally communicated by the Developer to SECI through written intimation along with a filled-out Project Execution Form (PEF), as per Annexure-D of the RfE. - The PEF shall accurately detail the plant's installed capacity (MW), technology mix, geographic zone, count of IT/OT Assets etc to allow auditors to size the effort accurately. - The PEF shall be linked to the Project assets. In case of assets located at multiple locations under a single Project, the PEFs shall be filled out separately for each location. In case of Hybrid Projects with assets being co-located, only a single PEF shall be submitted. - In case of multiple Projects being required to be audited by a single Project Developer, PEFs shall be filled out separately for each Project, subject to sub-clause e above.	

		g. It is understood that under a single entity, multiple SPVs may own the respective Projects. In such cases, the Parent Company of such SPVs may submit a single requisition letter to SECI, annexing the individual SPV-level PEF corresponding to each Project.	
11.	6.2.A.	This RFQ will be circulated exclusively to the empanelled auditors in the specific Geographic Zone where the plant is located.	This RfQ will be circulated exclusively to the empanelled auditors in the specific Geographic Zone where the plant assets are located. In case of a plant comprising Project assets located in more than one Zone, the RfQ shall be circulated only to those Auditors who have been empanelled in the respective Zones. In case of non-availability of empanelled Auditors in the respective Zones to bid in the RfQ, the RfQ shall be issued to all the Auditors empanelled under the RfE.
12.	6.2.B.	Clause modified as follows: Bid Opening and L1 Discovery (a) Upon the closing of the window for submission of quotation, SECI shall evaluate the submitted financial bids. (b) The RfQ shall seek price bids separately for each PEF. The Assignment will be awarded to the auditor who submits the lowest financial bid (L1 Bidder). (c) In case the Project comprises multiple components, following rules shall apply: - In case of multiple components located at the same location, a single PEF shall be submitted. Accordingly, a single Auditor shall be awarded the work for auditing the entire Project. - In case of multiple components located at multiple locations, either within the same Zone or in multiple Zones, the PEFs shall be submitted separately by the RPD. The assignment of auditing such Project shall also be awarded to a single Auditor. In this case, the Auditor shall submit price bids separately for each Project and the Auditor quoting the lowest aggregate price against all the PEFs for the Project shall be awarded the assignment. For eg., in case a Project of 300 MW Hybrid capacity comprises 200 MW Solar at Location-1 and 300 MW Wind at Location-2, the PEFs shall be submitted separately for Location-1 (PEF-1) and Location02 (PEF-2). The price bids shall also be submitted separately for each PEF, by the same Auditor, i.e. Price-1 and Price-2. The Auditor quoting the lowest summation of Price-1 and Price-2 shall be awarded the assignment. - Thus, in all cases, a single Auditor shall audit a Project comprising multiple project components. (d) In case of multiple Auditors quoting the L1 Price, then the ranking among these Auditors shall be done as follows:	

		i. The Auditor who has secured highest marks in the technical/QBS marking during the empanelment under this RfE, shall be considered as L-1. ii. If there is also a tie among any of these Auditors, then draw of lots will be conducted to determine the successful Auditor.										
13.	7.3	The Plant Developer is required to submit an Advance Payment along with the Project Execution Form (PEF) as per Annexure-D to SECI before any audit assignment can be officially initiated or a Work Order issued to the Auditor.	The Plant Developer is required to submit an Advance Payment prior to issuance of the Work Order by SECI.									
14.	7.5	Clause modified as follows: Milestone-based payment schedule The total audit fee for any given assignment shall be disbursed to the empanelled Auditor in two (2) instalments of 30 and 70, mapped to the successful completion and acceptance of the following milestones: <table><tr><th>Milestone</th><th>Description</th><th>Payment Instalment</th></tr><tr><td>Milestone-1</td><td>First Findings Report (Non-Conformity Report)</td><td>30% of total audit fee</td></tr><tr><td>Milestone-2</td><td>Final Audit Report & Management Approval</td><td>70% of total audit fee</td></tr></table> Submission of Milestone Performance Report (MPR) by the RPD to SECI shall be a mandatory pre-condition for release of payment by SECI to the Auditor under both the above instalments.		Milestone	Description	Payment Instalment	Milestone-1	First Findings Report (Non-Conformity Report)	30% of total audit fee	Milestone-2	Final Audit Report & Management Approval	70% of total audit fee
Milestone	Description	Payment Instalment										
Milestone-1	First Findings Report (Non-Conformity Report)	30% of total audit fee										
Milestone-2	Final Audit Report & Management Approval	70% of total audit fee										
15.	7.6	New Clause Milestone Performance Report (MPR) and Release of Payment (a) Submission of MPR: Upon completion of each Milestone under a given Assignment, the Auditor shall submit the relevant deliverables to the Renewable Power Developer (RPD), along with a Milestone Performance Report (MPR) recording the scope executed, findings/deliverables submitted, and confirmation of completion of that Milestone. (b) RPD Review Period: The RPD shall review the deliverables and communicate its acceptance or refusal (with specific, written reasons for refusal) of the MPR within a maximum of ten (10) working days from the date of submission of the MPR by the Auditor. In case of acceptance of the MPR, the same shall be duly signed by the authorized signatory of the RPD and forwarded to SECI. (c) Deemed Acceptance: In case the RPD fails to communicate its acceptance or refusal of the MPR within the said ten (10) working days, the MPR shall be deemed to have been accepted by the RPD for all purposes under this RfE and the Work Order, including for release of payment by SECI to the auditor for the respective Milestone.										

		(d) Refusal of MPR: In case the RPD refuses to accept the MPR within the ten (10) working-day period, it shall specify in writing the specific deficiencies/grounds for refusal, with a copy of the same being sent to SECI. The Auditor shall address such deficiencies and resubmit the MPR, and the RPD's review period under sub-clause (b) above shall apply afresh to such resubmission. A refusal that does not specify clear, assignment-related deficiencies, or that is not issued within the prescribed period, shall not be valid and shall not displace the deemed-acceptance provision at sub-clause (b) above. SECI's decision with respect to the grounds of refusal of MPR shall be final and binding on both parties. (e) Release of Payment: Payment of the respective Milestone instalment shall be released by SECI only upon (i) acceptance of the MPR by the RPD (whether express, under sub-clause (b), or deemed, under sub-clause (c)), and (ii) submission of the signed MPR (or, in case of deemed acceptance, the Auditor's MPR together with documentary proof of the date of submission to the RPD and expiry of the review period without refusal) to SECI. (f) Delay attributable to the RPD's non-response, non-cooperation, or unreasonable/invalid refusal under this Clause shall not be treated as a default on the part of the Auditor under this RfE and shall be reckoned as a factor outside the Auditor's reasonable control.
16.	8	Clause Modified as follows: <i>Performance Governance and Default Framework</i> 8.1 Assignment Completion Timeline (a) The entire audit assignment under a Work Order comprising both Milestone 1 and Milestone 2 shall be completed within a maximum period of 90 days from the date of issuance of the Work Order. For eg., in case the Work Order has been issued on 10.12.2026, the deadline for completion of the assignment shall be 10.03.2027. (b) The above timeline may be extended by SECI in writing, on a case-by-case basis, where the delay is attributable to the Plant Developer, its O&M contractor/OEM, SECI, delayed site access, delayed information, delayed patching, non-availability of required plant personnel, force majeure, or any other cause outside the Auditor's reasonable control, provided the Auditor furnishes prompt, formal written intimation of such cause and its impact on the schedule. (c) Failure to complete the assignment within the prescribed period as per sub-clause (a) above, where not covered by a permissible extension under sub-clause (b) above, shall constitute a milestone delay for the purposes of this Clause 8. 8.2 Delay and associated Liquidated Damages (LD) In case of delay beyond the timelines for completion of the Assignment as stipulated at Cl. 8.1 above, the Auditor shall be liable for Liquidated Damages as follows: i. LD shall be levied @5% of the total amount payable under the Work Order, for each week of delay or a part thereof, subject to the maximum LD being 10% of the total amount payable under the Work Order.

- ii. In case the delay period exceeds 4 weeks beyond the deadline as per Clause 8.1, the Work Order shall stand terminated without any liabilities on both the parties (Auditor and the Auditee).
- iii. The Parties acknowledge and agree that the Liquidated Damages stipulated under this RfE represent a reasonable pre-estimate of the loss and inconvenience likely to be suffered by the Auditee on account of delay attributable to the Auditor in completion of the Work or submission of the specified deliverables within the timelines prescribed under the Work Order. The Parties further acknowledge that the actual loss arising from such delay may be difficult to precisely ascertain or quantify at the time of breach. Accordingly, the Auditee shall be entitled to recover the Liquidated Damages stipulated under the Work Order upon occurrence of the relevant delay, without being required to separately demonstrate or quantify the actual loss suffered as a consequence thereof, subject to applicable law.
- iv. In case of termination of Work Order under sub-clause (ii) above, the assignment may be re-tendered by SECI, based on consultations with the RPD. In such case, the Auditor whose work order was terminated under sub-clause (ii) above, shall be debarred from bidding in such re-tender issued by SECI.

8.3 Event of Default

The occurrence of any of the following events during the empanelment period, unless any such event occurs as a result of Force Majeure or as breach by SECI or the RPD, shall constitute an Auditor's Event of Default:

- i. Declining SECI's Assignment allocations for the fourth time or refusal under Clause 8.5.i below, without due acceptance/condonation by SECI of such refusal.
- ii. Termination of work order by SECI under Clause 8.2 for the third time during the empanelment period.
- iii. Executing unauthorized active OT scanning or intrusive testing on live SCADA networks without written authorization from the Plant Operator's CISO and/or Plant Head.
- iv. Breaching data confidentiality protocols or failing to declare a conflict-of-interest post-assignment award.
- v. Failing to maintain a valid CERT-In empanelment.
- vi. Submitting forged, simulated, or fabricated audit evidence.

8.4 Procedure in case of Event of Default

In case the Event of Default is triggered by any of the events as per Clause 8.3 above, the Auditor shall be removed from the empanelled list of Auditors by SECI under this RfE, with no further payments to be released to the Auditor under any Work Order being in force at that stage.

8.5 SECI's Discretion in Exigency and Untoward Incidents

i. **Overriding Discretion:** Notwithstanding anything contained in this RfE, SECI, in its capacity as CERT-RE, reserves the absolute discretion to engage any empanelled Auditor, whether empanelled in the Geographic Zone in which the plant is situated or in any other Geographic Zone, for any assignment, without recourse to the zonal Request for Quotation process, in any of the circumstances set out as follows:

- a. a cyber security incident, suspected incident, breach, intrusion, ransomware event, data compromise or attempted compromise has occurred or is apprehended at any RE plant or across the RE sector, requiring urgent assessment, containment support or forensic examination;
- b. a direction, advisory or requisition has been received from CERT-In, CSIRT-Power, NCIIPC, CEA, MNRE, the Ministry of Power, GRID-India or any other competent authority requiring audit, verification or assessment within a stipulated timeline;
- c. no quotation, or an inadequate number of quotations, is received in response to a Request for Quotation issued in the relevant Zone or for the respective PEFs, or the quotations received are considered by SECI to be unreasonable;
- d. the Auditor to whom a Work Order has been issued is de-empanelled/becomes ineligible/is in default/is otherwise unable or unwilling to complete the Assignment;
- e. applying the process under Clause 6 would result in the plant failing to meet a statutory audit timeline under the Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2026;
- f. the rotation restriction under Clause 3.3 (no more than three consecutive audits by the same Auditor) or a declared conflict of interest exhausts the pool of eligible Auditors in the relevant Zone;
- g. the assignment requires specialised technology, protocol or OEM-specific competency not available among the Auditors empanelled in the relevant Zone;
- h. any other exigency, force majeure event, natural calamity, sabotage, grid disturbance or untoward incident which in SECI's opinion warrants departure from the standard selection process.

ii. **Obligation to Accept:** An Auditor engaged under Clause 8.5.i shall mandatorily accept the Assignment awarded by SECI and accordingly mobilise at the earliest. Refusal or non-mobilisation otherwise than as permitted shall constitute a default under Clause 8.3 and shall additionally render the Auditor liable to the procedure as per Clause 8.4. An Assignment declined with SECI's acceptance under this Clause shall not be counted as a declined allocation for the purposes of Clause 8.3.

8.6 **Confidentiality of Incident Engagements:** Engagements under Clause 8.5.i shall be treated as confidential. The Auditor shall not disclose the fact, scope, findings or existence of such engagement to any person other than SECI.

		8.7 No Right Accrues: Nothing in this RfE confers on any Auditor any right, entitlement or expectation to be engaged, or to be considered for engagement. Empanelment does not guarantee any assignment. SECI's decision as to whether an exigency exists, which Auditor to engage, and on what terms, shall be final and binding on all empanelled Auditors and shall not be open to challenge. 8.8. Change Request Management a. The conditions stipulated in the Work Order, along with the awarded price under the Work Order shall be binding on the Auditor, with no revisions acceptable under normal conditions. However, in case of occurrence of any of the following events, the Auditor shall be eligible to claim a revision of the Work Order's terms under Change Request Management (CRM): i. Increase in the actual asset count more than 15% of the total asset count indicated in the PEF. In case the Auditor is handling multiple PEFs under the same Project, the 15% limit shall be applied individually for each PEF. ii. Major enhancement in the Scope of Work for a particular assignment, which is not covered under the current scope of work under the RfE. b. In such cases, the revision in awarded price and timeline for completion of the assignment shall be mutually decided by SECI, RPD and the Auditor.	
17.	11.4	Subsequent to completion of initial empanelment period of 2 years, in case the empanelment period is extended by SECI, then the empanelled Auditor shall pay a nonrefundable annual Empanelment Fee of INR 10,000/- (Indian Rupees Ten Thousand only) plus 18% GST per Zone per year to SECI.	Subsequent to completion of initial empanelment period of 2 years, in case the empanelment period is extended by SECI, then the empanelled Auditor shall pay a nonrefundable annual Empanelment Fee of INR 10,000/- (Indian Rupees Ten Thousand only) plus 18% GST per Zone per year to SECI. Delay in payment of this fee shall also be treated by the applicable provisions as per Clause 11.3.
18.	12	Clause modified as follows: <i>Non-Disclosure Agreement (NDA)</i> a. In case required by the Plant Developer, a Non-Disclosure Agreement (NDA) may be signed between the Auditor and the Auditee, as per the format mutually agreed between the two Parties. b. Notwithstanding the terms of the NDA, if any, provisions of Clause 4.2 shall be applicable on all audit assignments undertaken under this RfE.	
19.	13.2	 The auditing organization must demonstrate technical accuracy and structured methodology by deploying full-time professional experts who hold valid,	 The auditing organization must demonstrate technical accuracy and structured methodology by deploying minimum one full-time professional

		internationally recognized cybersecurity certifications.	expert who holds valid, internationally recognized cybersecurity certifications.
20.	14.iii.	Board Resolution, as per Format 7.3 duly certified by the Company Secretary or the Director of the relevant Bidder, as applicable to the Bidder in favour of the person signing the response to RfE and in the event of empanelment and to sign the NDA with SECI.	Board Resolution, as per Format 7.3 duly certified by the Company Secretary or the Director of the relevant Applicant, as applicable to the Applicant in favour of the person signing the response to RfE.
21.	17.1	 The Bidder will be required to submit the Offline Bid, either in person or through post, at the office of SECI until the date as on 2 working days after the closing date of Online bid submission. The 2-day duration will be counted from the date of Online bid submission. For e.g., if the bid submission deadline is 18:00 hrs on 25.09.2026, the above deadline will expire at 18:00 hrs on 27.09.2026. In case the above deadline being a holiday, the next working day in SECI will be the deadline for submission of Offline bid. ...	 The Applicant will be required to submit the Offline Bid, either in person or through post, at the office of SECI until the bid submission deadline. In case the above deadline being a holiday, the next working day in SECI will be the deadline for submission of Offline bid. ...
22.	22.3.b.	New bullet point added after the last bullet point Neither party will be responsible for any amount with respect to loss of profit, data or goodwill, or any other consequential, incidental, indirect, exemplary, punitive or special damages in connection with claims arising out of this Agreement or otherwise relating to the Services, whether or not the likelihood of such loss or damage was contemplated.	
23.	22.4	New Clause Force Majeure - A 'Force Majeure' means any event or circumstance or combination of events those stated below that wholly or partly prevents or unavoidably delays an Affected Party in the performance of its obligations under the Work Order, but only if and to the extent that such events or circumstances are not within the reasonable control, directly or indirectly, of the Affected Party and could not have been avoided if the Affected Party had taken reasonable care or complied with Prudent Utility Practices: - Act of God, including, but not limited to lightning, fire not caused by Auditor's negligence and explosion (to the extent originating from a source external to the site), earthquake, volcanic eruption, landslide, unprecedented flood, cyclone, typhoon or tornado;	

		ii. Any act of war (whether declared or undeclared), invasion, armed conflict or act of foreign enemy, blockade, embargo, revolution, riot, insurrection, terrorist or military action, quarantine; iii. Radioactive contamination or ionizing radiation originating from a source in India or resulting from another Force Majeure Event mentioned above. b. Force Majeure Exclusions Force Majeure shall not include (i) any event or circumstance which is within the reasonable control of the Parties and (ii) the following conditions, except to the extent that they are consequences of an event of Force Majeure: i. Delay in the performance of any Auditor or its agent(s); ii. Non-performance resulting from normal wear and tear typically experienced in power generation materials and equipment/Service; iii. Strikes at the facilities of the Auditor / Affected Party; iv. Insufficiency of finances or funds or the Assignment becoming onerous to perform; v. Non-performance caused by, or connected with, the Affected Party's: a. Negligent or intentional acts, errors or omissions; b. Failure to comply with an Indian Law; or c. Breach of, or default under this Contract Agreement. vi. Normal rainy seasons and monsoon vii. Any Transport strikes not directly affecting the access to the Project site c. In the event of either party being rendered unable by Force Majeure to perform any obligation required to be performed by them under the Work Order, relative obligation of the party affected by such Force Majeure shall be treated as suspended during the period which the Force Majeure persists. d. Upon occurrence of such causes, the party alleging that it has been rendered unable as aforesaid, thereby, shall notify the other party in writing by registered notice within 7 (Seven) Days of the alleged beginning thereof giving full particulars and satisfactory evidence in support of its claim. Further, within 14 (Fourteen) days, the Auditor will furnish a detailed Contingency Plan to overcome the effects of the incident and bring the Assignment on its schedule after cessation of the effect of Force Majeure. e. The Affected Party shall give notice to the other Party of (i) the cessation of the relevant event of Force Majeure; and (ii) the cessation of the effects of such event of Force Majeure on the performance of its rights or obligations under the Work Order, as soon as practicable after becoming aware of each of these cessations. f. Time for Performance of the relative obligation suspended by the force majeure shall stand extended by the period for which such Force Majeure event lasts. g. If the assignment-related activities are suspended by Force Majeure conditions lasting for more than two months, the SECI, at its discretion, shall have the option
--	--	---

		of cancelling the Work Order in consultation with the respective RPD, in whole or part thereof. h. The Auditor will not be entitled to claim any compensation for Force Majeure conditions and shall take appropriate steps to insure its men and materials utilized by it under the Work Order. i. To the extent not prevented by force majeure event, the affected party shall continue to perform its obligations pursuant to this Agreement. The Affected Party shall use its reasonable efforts to mitigate the effect of any Force Majeure Event as soon as practicable.	
24.	23	PQ-3 Documentary Proof: Work Order (WO) / Purchase Order (PO)/ LoA along with Performance Certificate / Completion Certificate/ Successful Order execution confirmation from client.	PQ-3 Documentary Proof: Work Order (WO) / Purchase Order (PO)/ LoA along with Performance Certificate / Completion Certificate/ Successful Order execution confirmation from client/Certificate from a practicing Chartered Accountant (CA), certifying the completion of the assignment along with proof of payment of the final bill/invoice.
25.	23	Addition of a new entry in the table PQ-5: Minimum Average Annual Turnover (MAAT) of the Bidder in the last three Financial Years, i.e. 2023-24, 2024-25 and 2025-26, should be INR 50,00,000 (Indian Rupees Fifty Lakhs only)	
26.	24	Table Modified as per Annexure-II	
27.	27.2	The bidders securing at least 70 marks shall be empaneled in the Geographic Zones applied for in Format 7.1.	The bidders securing at least 70 marks shall be declared as “Successful Bidders” and will be eligible to be empanelled by SECI in the respective Geographic Zones as applied for in Format 7.1.
28.	29.3	“ BID ” or “ PROPOSAL ” shall mean the documents submitted by the Bidder towards meeting the technical and financial qualifying requirements....	“ BID ” or “ PROPOSAL ” or “ APPLICATION ” shall mean the documents submitted by the Bidder towards meeting the technical and financial qualifying requirements....
29.	29.4	“ BIDDER ” shall mean Bidding Entity submitting the Bid. Any reference to the Bidder includes Bidding Entity including its successors, executors and permitted assigns, as the context may require;	“ BIDDER ” or “ APPLICANT ” shall mean Bidding Entity submitting the Bid. Any reference to the Bidder includes Bidding Entity including its successors, executors and permitted assigns, as the context may require. It is clarified that the “Bidder” under this RfE is different

			from the “Bidders” submitting their quotations under the RfQ issued by SECI in Stage-II of this RfE;
30.	29.29	“PROJECT” shall mean the Renewable Energy Project developed by the Renewable Power Developer	“PROJECT” or “PLANT” shall mean the Renewable Energy Project developed by the Renewable Power Developer, whose assets are to be audited under this RfE;
31.	29.30	“PROJECT DEVELOPER” or “DEVELOPER” or “RENEWABLE POWER DEVELOPER” shall mean the Entity which has developed the Renewable Energy Project	“PROJECT DEVELOPER” or “DEVELOPER” or “RENEWABLE POWER DEVELOPER” or “RPD” shall mean the Entity which has developed the Renewable Energy Project, whose assets are to be audited under this RfE;
32.	29.35	“SOLAR PV PROJECT” or “SOLAR POWER GENERATING SYSTEM/STATION” shall mean the Solar Photo Voltaic Power Project that uses sunlight for direct conversion of solar energy into electricity through Photo Voltaic Technology	“RE PROJECT” or “Renewable Energy Project” shall mean a Solar/Wind/Hybrid/Pumped Storage Project, with or without Battery Energy Storage Systems (BESS), using solar/wind/hydro power or a combination thereof, to generate energy.
33.	29.39	New Clause “WORK ORDER” shall refer to the award of work issued by SECI under Stage-II of this RfE, to the selected Auditor, corresponding to a specific Project/Assignment.	
34.	Annexure - C	Not used	
35.	Annexure -D	Modified as per Annexure-III	

Clause 4. Mandatory Execution Milestones & Deliverables

4.1 The Auditor shall execute the assignment in clear, distinct project phases as defined below:

Milestone	Project Phase	Key Activities & Verification Parameters
Milestone-1: First Findings Report (Non-Conformity Report)	<u>Phase A:</u> Mobilization & Planning	• Initiate project kick-off and validate the audit scope checklist. • Request initial governance documents (Cyber Security Policy, C-CMP, ISO 27001 certificates, CISO appointment details). • Schedule the physical on-site inspection visit. Deliverables: Project Kick off report and audit plan
	<u>Phase B:</u> Asset Discovery	• Check all IT and OT plant assets as listed out in the PEF, compiling hardware/software inventories and OEM details. • Verify zone diagrams, asset-to-zone mapping tables, and the physical/logical isolation between IT and OT systems.
	<u>Phase C:</u> Full-Stack Cybersecurity Audit	• Conduct physical site inspections for server/control room access and operations security. • Review firewall configurations, default-denied rules, and advanced security technologies (e.g., DPI, WAF, EDR). • Execute Vulnerability Assessment and Penetration Testing (VAPT) across IT systems and test IT-to-OT lateral movement paths. • Strict Constraint: Strict Constraint: Ensure no unauthorized active OT scanning or intrusive testing occurs on live SCADA networks without written approval from the Plant Head and CISO.
	<u>Phase D:</u> Analysis & Report Preparation and Submission	• Consolidate all physical verification, documentation review, and VAPT results. • Document identified security flaws, non-compliances, and risk ratings. Deliverables: Submission of Initial Vulnerability & Non-Compliance Report of Audit Checklist (Annexure B)
Milestone 2: Final Audit Report & Management Approval	<u>Phase E:</u> ATR Review & Re-Audit Preparation	• Receive and evaluate the Action Taken Report (ATR) submitted by the Plant Developer in response to Phase D findings. • Formally review the remediation measures implemented against the initial non-conformities. Deliverable: Approved Re-scan schedule
	<u>Phase F:</u> Re-Audit / Re-Scan	• Conduct targeted differential scanning and re-testing to verify the successful closure of previously identified vulnerabilities.

		• Confirm patches have been applied and configurations corrected. Deliverable: Retest Audit Report
	Phase G: Consolidated Draft Report Preparation	• Compile the comprehensive draft report combining initial findings, remediation actions, and final re-scan results. • Complete regulatory compliance mapping (e.g., CEA regulations, CERT-In directives, IT Act). Deliverable: Draft Audit Report
	Phase H: Plant Developer Management Review	• Conduct an executive management briefing and review session with the Plant's CISO and Top Management. • Discuss residual risks, if any, and obtain alignment on the final findings. Deliverable: Management consensus and sign-off on the draft report. SECI may be a part of this review, if required.
	Phase I: Final Submission and Closure	• Auditor to issue the finalized Cybersecurity Audit Report and Vulnerability Closure Report. • Auditor to provide formal compliance certificate to the Auditee based on compliance with the checklist as per Annexure-B of the RfE.

- 4.2 The reports generated/findings under the above milestones or as part of the Assignment shall mandatorily be made available by the Auditor to SECI through email or uploading the same on a portal as identified by SECI. By sharing the reports with SECI, the Auditor expressly grants its consent to SECI for sharing of these documents by SECI with other Government Agencies/Regulators as and when required under the applicable Rules/Regulations from time to time.
- 4.3 Normally, a single round of retest/re-scan is envisaged under Phase-F after completion of Milestone-1, and the same can be carried out remotely, if feasible. Subsequent rounds of retesting/re-scan, if any, requiring major tasks to be carried out, may be considered under Change Request, based on mutual discussions between SECI, RPD and the Auditor.

Revised Quality Based Selection Criteria

Sl. No.	Criteria	Documentation required	Max Marks	Criteria for Scoring												
C1	Average Annual Turnover of the last three Financial Years (FY 2023-24, 2024-25, 2025-26)	Audited Financial Statements/ Certificate from a Practicing Chartered Accountant (CA).	10	<table><tr><th>MAAT (“X” in Rs. Cr.)</th><th>Marks</th></tr><tr><td>$0.5 \leq X < 5$</td><td>3</td></tr><tr><td>$5 \leq X \leq 10$</td><td>5</td></tr><tr><td>$X > 10$</td><td>10</td></tr></table>	MAAT (“X” in Rs. Cr.)	Marks	$0.5 \leq X < 5$	3	$5 \leq X \leq 10$	5	$X > 10$	10				
MAAT (“X” in Rs. Cr.)	Marks															
$0.5 \leq X < 5$	3															
$5 \leq X \leq 10$	5															
$X > 10$	10															
C2	<u>Auditing Organization Experience:</u> Number of years the bidder has been engaged in the field of cybersecurity, especially in cybersecurity audits, is an indicator of technical exposure, knowledge, and understanding in identifying and addressing cybersecurity risks.	Work Order (WO) / Purchase Order (PO)/ LoA along with Performance Certificate / Completion Certificate/ Successful Order execution confirmation from client/ practicing Chartered Accountant-certified statement validating years of cybersecurity experience, along with proof of payment of final invoice/bill.	20	<table><tr><th>Cybersecurity Experience (‘X’ in years)</th><th>Marks</th></tr><tr><td>$5 < X$</td><td>20</td></tr><tr><td>$3 < X \leq 5$</td><td>15</td></tr><tr><td>$1 < X \leq 3$</td><td>10</td></tr><tr><td>$0 < X \leq 1$</td><td>5</td></tr><tr><td>Nil</td><td>0</td></tr></table>	Cybersecurity Experience (‘X’ in years)	Marks	$5 < X$	20	$3 < X \leq 5$	15	$1 < X \leq 3$	10	$0 < X \leq 1$	5	Nil	0
Cybersecurity Experience (‘X’ in years)	Marks															
$5 < X$	20															
$3 < X \leq 5$	15															
$1 < X \leq 3$	10															
$0 < X \leq 1$	5															
Nil	0															
C3	<u>Technical Manpower Expertise:</u> The bidder shall have certified professionals on the company payroll, having any of the following valid certifications: CISSP, CISM, CISA, IEC 62443, ISO 27001 Lead Auditor, CEH, OSCP, GICSP, ISO 27001 LI.	Copies of relevant certifications for each of the employees; Documentary proof of full-time employees holding valid certifications which can include appointment letters/ employment proofs confirming payroll status/ certificate issued by authorised signatory on the Bidder’s letterhead.	15	<table><tr><th>No. of Certified Professionals (‘X’)</th><th>Marks</th></tr><tr><td>$20 \leq X$</td><td>15</td></tr><tr><td>$10 \leq X < 20$</td><td>12</td></tr><tr><td>$5 \leq X < 10$</td><td>8</td></tr><tr><td>$0 < X < 5$</td><td>4</td></tr><tr><td>Nil</td><td>0</td></tr></table>	No. of Certified Professionals (‘X’)	Marks	$20 \leq X$	15	$10 \leq X < 20$	12	$5 \leq X < 10$	8	$0 < X < 5$	4	Nil	0
No. of Certified Professionals (‘X’)	Marks															
$20 \leq X$	15															
$10 \leq X < 20$	12															
$5 \leq X < 10$	8															
$0 < X < 5$	4															
Nil	0															

C4	Number of Cybersecurity Audits in Last Three Years: This criterion assesses the frequency of cybersecurity audit engagements, enabling the organization to stay updated with the latest regulatory requirements, evolving threat landscapes, and emerging security technologies.	Work Order (WO) / Purchase Order (PO)/ LoA along with Performance Certificate / Completion Certificate/ Successful Order execution confirmation from client/ practicing Chartered Accountant-certified statement for completed cybersecurity audits in the last three years, along with proof of payment of final invoice/bill.	15	<table><tr><th>No. of Audits in Last 3 Years ('X')</th><th>Marks</th></tr><tr><td>20≤X</td><td>15</td></tr><tr><td>10≤X<20</td><td>12</td></tr><tr><td>5≤X<10</td><td>8</td></tr><tr><td>0<X<5</td><td>4</td></tr><tr><td>Nil</td><td>0</td></tr></table>	No. of Audits in Last 3 Years ('X')	Marks	20≤X	15	10≤X<20	12	5≤X<10	8	0<X<5	4	Nil	0
No. of Audits in Last 3 Years ('X')	Marks															
20≤X	15															
10≤X<20	12															
5≤X<10	8															
0<X<5	4															
Nil	0															
C5	Certifications for Recognized Standards: The bidder shall possess valid certifications for recognized standards, demonstrating commitment to global standards and best practices. <u>Required certifications:</u> — ISO/IEC 27001 (Information Security Management System) — Mandatory — ISO 9001 (Quality Management System) — ISO 20000 (IT Service Management) — ISO/IEC 17021 or ISO/IEC 27006 (where applicable)	Valid certificates from accredited certification bodies. ISO 27001 is mandatory. ISO 9001, ISO 20000, ISO 27006 certificates to be submitted where held.	10	<table><tr><th>Certifications Held</th><th>Marks</th></tr><tr><td>All four</td><td>10</td></tr><tr><td>Any three</td><td>6</td></tr><tr><td>Any two</td><td>4</td></tr><tr><td>ISO 27001 only</td><td>2</td></tr></table>	Certifications Held	Marks	All four	10	Any three	6	Any two	4	ISO 27001 only	2		
Certifications Held	Marks															
All four	10															
Any three	6															
Any two	4															
ISO 27001 only	2															

C6	Additional Criteria for OT System Cybersecurity Audit — Project Experience in OT Systems: This criterion evaluates the project experience of the auditing organization in Operational Technology (OT) systems, ensuring that organizations have the necessary experience to effectively assess and secure OT systems in accordance with industry standards.	Work Order (WO) / Purchase Order (PO)/ LoA along with Performance Certificate / Completion Certificate/ Successful Order execution confirmation from client/ practicing Chartered Accountant-certified statement, evidencing OT domain cybersecurity project experience/ identification of sector of the auditee entity, along with payment proof of the final bill/invoice.	20	<table><tr><th>OT Domain Experience (‘X’ years)</th><th>Marks</th></tr><tr><td>7≤X</td><td>15</td></tr><tr><td>3≤X<7</td><td>10</td></tr><tr><td>0<X<3</td><td>5</td></tr><tr><td>Nil</td><td>0</td></tr></table> Additional 05 marks to be awarded having for demonstrating successful completion of minimum 01 Power/Energy Sector assignment under the OT domain experience.	OT Domain Experience (‘X’ years)	Marks	7≤X	15	3≤X<7	10	0<X<3	5	Nil	0
OT Domain Experience (‘X’ years)	Marks													
7≤X	15													
3≤X<7	10													
0<X<3	5													
Nil	0													
C7	Additional OT System Specific Criterion — Availability of Technical Experts in the OT Domain: This criterion evaluates the availability of technical expertise and experience of personnel in the OT domain, particularly with systems such as SCADA, Distributed Control Systems (DCS), and Substation Automation Systems (SAS), ensuring the auditing organization has qualified personnel capable of conducting audits of deployed OT systems.	CVs and certifications of OT-qualified personnel (IEC 62443, SIL, or equivalent); For employment proof: appointment letters/ employment proofs confirming payroll status/ certificate issued by authorised signatory on the Bidder’s letterhead	10	<table><tr><th>No. of Experienced manpower (‘X’)</th><th>Marks</th></tr><tr><td>5≤X</td><td>10</td></tr><tr><td>3≤X<5</td><td>8</td></tr><tr><td>1≤X<3</td><td>5</td></tr><tr><td>X<1</td><td>3</td></tr></table>	No. of Experienced manpower (‘X’)	Marks	5≤X	10	3≤X<5	8	1≤X<3	5	X<1	3
No. of Experienced manpower (‘X’)	Marks													
5≤X	10													
3≤X<5	8													
1≤X<3	5													
X<1	3													
Total			100											

Note: If a single Work Order submitted above covers more than one Project, then each Project covered under such Work Order will be counted separately for the purpose of demonstrating the requisite experience (The work order should clearly establish the number of projects covered).

Modified Project Execution Form (Annexure-D of the RfE)

		Solar Energy Corporation of India Limited <i>(A Navratna Government of India Enterprise)</i> Ministry of New and Renewable Energy Sectoral Computer Emergency Response Team for the Renewable Energy Sector (CERT-RE), New Delhi		
PROJECT EXECUTION FORM (PEF)		PEF No.: <i>(To be filled by SECI)</i>	Date: / /	
Requisition for Mandatory Cyber Security Audit of a Renewable Energy Plant under CEA Cyber Security Regulations, 2026, in line with the provisions of RfE document issued by SECI vide RfE No. SECI/C&P/EOI/17/0004/26-27 dated 28.08.2026				
(A) Developer Details				
1	Name of the Renewable Power Developer (RPD)			
2	CIN / LLPIN		GSTIN:	
3	Registered Address			
(B) Plant Details				
1	Name of the Tender, if awarded by REIA or any Buying Entity			
2	LoA Number (if applicable)			
3	Project Type (Solar PV / Wind / Hybrid (Co-located/ multi-located) / BESS / RE with BESS)			
4	Installed Capacity (In case of co-located hybrid or RE with co-located BESS, these details need to be filled out separately for each component i.e. Solar, Wind, BESS)	AC (MW):	DC (MWp):	BESS (MW/MWh):
5	Location of Plant assets (In case of multi-located plant assets under single project, PEF has to be	Village/Tehsil: District:		

	filled out separately for each location)	State/UT: Geographic Zone as per RfE(1 to 5): Geo-Coordinates (latitude, longitude):		
6	Date of Commercial Operation / Scheduled COD	COD:	Manning: manned / partly / unmanned	
7	Grid Connectivity	ISTS / InSTS:	Substation and voltage (kV):	
8	SLDC / RLDC / REMC interface	Entity:	Protocol:	
9	Declared a Protected System under Section 70 of the IT Act, 2000? (Yes / No)			
10	Operation and Maintenance	Self / third party:	Name of O&M contractor:	
(C) Audit Trigger and Audit History				
1	Type of Audit requisitioned (Choose one)	First Time Charge (FTC)	Periodic Mandatory Audit	
3	In case of Periodic Audit	Audit cycle no.:	Due date (As per CEA Regulations, 2026):	
4	Details of the preceding audit	Name of auditing organisation:	Closure date:	Consecutive audits by same auditor:
5	Open non-conformities from preceding audit (fill in detail)	Critical / High:	Medium / Low:	
6	Any cyber security incident reported to CERT-In / CERT-RE / CSIRT-Power in the preceding twelve months (Yes / No — reference and date)			
7	Preferred audit window (from / to)	DD/MM/YYYY		
(D) Cyber Security Governance and Documentation Readiness				
1	Chief Information Security Officer (CISO)	Name:	Designation:	
		Email:	Phone/Mobile:	
2	Information Security Division	Constituted (Yes / No):	Date of constitution:	
3	Cyber Security Policy	Approved (Yes / No):	Version and date:	

4	ISO/IEC 27001 certification	Certificate no.:	Validity:
5	Availability of records	Asset register / CMDB (Yes / No):	Network architecture diagram (Yes / No):
6	Supply chain declarations	Trusted-source / MoP lab certificates (Yes / No / Partial):	SBOM available (Yes / No / Partial):

(E) Asset Summary

Type-wise asset counts shall be furnished in Annexure-I and Annexure-II. Enter totals only in this Part.

1	IT Assets — Appendix-I	Total count:	Assets to be audited:
2	OT / ICS Assets — Appendix-II	Total count:	Assets to be audited:
3	GRAND TOTAL		

(F) Network, Connectivity and Remote Access

1	IT / OT segregation (air-gapped / firewalled with DMZ / firewalled without DMZ / flat)	
2	Is standing OEM / vendor remote access enabled for any OT asset? (Yes / No — list assets and OEMs)	

(G) Site Logistics and Access

1	Nearest transit points	Airport and distance (km):	Railway station and distance (km):
2	Site SPOC	Name:	Designation:
		Email:	Phone/Mobile:
3	IT SPOC	Name:	Designation:
		Email:	Phone/Mobile:
4	OT SPOC	Name:	Designation:
		Email:	Phone/Mobile:

UNDERTAKING

We certify that the particulars furnished herein, including the asset counts at Annexure-I and Annexure-II, are true, complete and correct as on the date of submission. We understand that these counts form the basis on which the audit effort is scoped and the audit fee is discovered, and that any material understatement shall entitle SECI to revise the fee, to require the assignment to be re-scoped, or to report the matter to the Central Electricity Authority. We undertake to furnish all governance documents, architecture diagrams, asset registers, configuration data, logs and access required for the audit; to grant timely site access and escorted access to control rooms, server rooms, inverter stations and substation premises; to ensure the availability of the officers named at Parts D and G; not to require or permit the Auditor to conduct any active or intrusive testing on live process control networks without our prior written authorisation issued jointly by the Project In-charge and the CISO; and to submit the Action Taken Report within the timeline. We accept that the audit is a point-in-time assessment and that a closure certificate does not constitute a warranty against future cyber-attacks, zero-day

vulnerabilities or subsequent intrusions.

Certified by

Signature and stamp:

Name:

Designation: Chief Information Security Officer

Date:

For and on behalf of the Renewable Power Developer

Signature and stamp:

Name:

Designation: Authorised Signatory

Date:

* The PEF must be signed by the authorised signatory of the Developer and countersigned by the CISO.

* All fields are mandatory. Where not applicable, enter "NA". An incomplete PEF shall be returned.

APPENDIX-I: IT ASSETS

State the total number of each asset type deployed at all locations forming part of the audit scope.

S. No.	Asset type	Count (A)	Min Sampling rate (B)	Assets to be audited (C=A*B)	Make / OEM and remarks
1	Servers (physical and virtual)		0.50		
2	Desktops / Laptops (endpoints)		0.25		
3	Firewalls (IT)		1.00		
4	IDS / IPS appliances		1.00		
5	Routers		0.50		
6	Switches		0.50		
7	Wireless Access Points / Controllers		0.25		
8	CCTV / IP cameras and NVR		0.25		
9	Networked printers / MFPs		0.25		
10	Public-facing IP addresses		1.00		
11	Web / ERP applications (for PT)		1.00		
12	Mobile applications (for PT)		1.00		
13	APIs (for PT)		1.00		
	Sub-total — IT assets				

Certified by

Signature and stamp:

Name:

Designation: Chief Information Security Officer

Date:

APPENDIX-II: OT / ICS ASSETS

S. No.	Asset type	Count (A)	Min. Sampling rate (B)	Assets to be audited (C=A*B)	Make / OEM and remarks
1	SCADA / EMS / DCS servers		1.00		
2	HMI stations		0.25		
3	Engineering workstations (EWS)		0.25		
4	Historian / Data-logger servers		1.00		
5	Power Plant Controllers (PPC)		1.00		
6	PLCs		0.50		
7	RTUs		0.50		
8	Protection relays / IEDs		0.50		
9	Bay controllers		0.50		
10	Substation gateways / IEC 61850 devices		0.50		
11	GPS / Time-sync (PTP / NTP) devices		0.25		
12	ABT / Special Energy Meters		0.25		
13	String inverters		0.10		
14	Central inverters		0.10		
15	Smart combiner boxes (monitored)		0.10		
16	Tracker controllers		0.10		
17	Weather / Pyranometer stations (networked)		0.10		
18	WTG controllers		0.10		
19	Condition-monitoring systems		0.10		
20	Met masts (networked)		0.10		
21	Battery Management Systems (BMS)		0.10		
22	Power Conversion Systems (PCS)		0.10		
23	Battery EMS units		0.10		
24	OT firewalls / data diodes / unidirectional gateways		1.00		
25	Jump servers / bastion hosts (OT)		0.50		
	Sub-total — OT / ICS assets				
	GRAND TOTAL — IT and OT / ICS				

Sampling methodology applied by SECI: 100% for unique and high-consequence assets (SCADA and EMS servers, firewalls, historians, public IP addresses, and all applications and APIs subjected to penetration testing); 50% for role-varied infrastructure (servers, routers, switches, PLCs, RTUs, relays, bay controllers); 25% for endpoints and semi-identical devices (desktops, HMIs, engineering workstations, cameras, meters); 10% for factory-identical field fleets (inverters, tracker controllers, WTG controllers, BMS and PCS units) — in every case subject to a minimum of two units per asset type and capped at the declared count. Payable assets per row = ROUNDUP (Count × Sampling rate).

Certified by

Signature and stamp:

Name:

Designation: Chief Information Security Officer

Date:

FOR SECI's INTERNAL USE ONLY

1	PEF received on (date)	
2	PEF reference number allotted	
3	Completeness check — complete / returned for rectification	
4	Advance payment realisation confirmed on (date)	
5	Total payable assets computed (IT / OT / total)	
6	Geographic Zone confirmed	
7	Auditors excluded on rotation or conflict-of- interest grounds	
8	RFQ issued on (date) and RFQ reference	
9	Verified by (name, designation, signature)	