

भारत हेवी इलेक्ट्रिकल लिमिटेड
Bharat Heavy Electricals Limited



कॉर्पोरेट डिजिटल ट्रांसफॉर्मेशन
CORPORATE DIGITAL TRANSFORMATION

**CDT, 2nd Floor, HRDI Building, BHEL HRDI & ESI Complex, Plot No-25, Sector-16A,
Noida -201301**

Request for Proposal

FOR

**“Hiring of services of Centre for Development of Advanced Computing (C-DAC), Ministry of
Electronics and Information Technology (MeitY) for security audit of Application System**

Ref. No. AA: CDT: ACS:CPS-Audit dtd. 20.09.2025

To be signed and stamped by the bidder

Page 1

Scope of Work (SOW):

Summary of the SOW is as below:

- 1.1 BHEL uses an application hosted on intranet wherein the details of payment vouchers are posted by various BHEL Units and later processed centrally for payment. Some Inconsistencies were observed in this transactional system in Jan 2025
- 1.2 BHEL proposes to perform an independent assessment of the incident, conduct a root cause analysis of the lapse and identify process gaps, system vulnerabilities and IT Policy violations in development of the application and within the payment function.
- 1.3 The key objectives of the proposed engagement are list below :
 - 1.3.1 Conduct a detailed analysis of the end-to-end processes of payments, with a focus on voucher batching and payment processing, to identify gaps which caused the Inconsistency.
 - 1.3.2 Evaluate vulnerabilities or violations within IT system, alongside an in-depth review of internal controls, to understand their contribution to the issue.
 - 1.3.3 Identify systemic deficiencies and provide actionable recommendations to strengthen the control environment and minimize future risks.
 - 1.3.4 Evaluate the instance of inconsistencies to find out violation of checks and balances and policies, vulnerabilities within the system and normal standards of prudence at different stages leading to inconsistencies.

1.4 **Table 1: Milestones & deliverables**

Milestone	Description of Scope	Bidder Compliance (Yes/No)	Bidder Remarks
	The entire scope of work and deliverables covered in this document and subsequent instructions to Bidder by the Owner post award shall be deemed to be Bidder's obligation.		
M1	a) Application Development / Implementation Review i. BHEL has implemented		

Ref. No. AA: CDT: ACS:CPS-Audit dtd. 20.09.2025

To be signed and stamped by the bidder

Page 2

	<p>Information Security Management System (ISMS) and is ISO 27001:2022 certified by STQC, Ministry of Electronics & Information Technology (MeitY). A study of the Information Security Management System & all relevant policies and procedures of BHEL.</p> <p>ii. A report on the implementation of the Information Security Policies / Procedures in the development / implementation of the updated version of the Application and its rollout beyond Corporate Office around H2 of CY 2024.</p> <p>iii. A report on the types of Roles created, their methodology, user creation, user rights allocation and review of the user access rights, intended as well unintended. Access rights / permissions to be reviewed.</p> <p>iv. A report of password policy implementation and the cryptography used in passwords.</p> <p>v. A report on various types of Application logs configured, generated and their relevance, including such logs that were required to trace any data manipulation or to conduct root cause analysis of any undesirable incident, but were not provided.</p> <p>vi. A report on Change Management process followed during any changes and during the roll-out of the Application beyond Corporate Office in H2 of CY 2024.</p> <p>b) Application Code Review</p> <p>i. Application Code for the updated version implemented in H2 of CY</p>		
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

Ref. No. AA: CDT: ACS:CPS-Audit dtd. 20.09.2025

To be signed and stamped by the bidder

Page 3

	<p>2024 to be checked for Compliance of the functional requirements.</p> <ul style="list-style-type: none"> ii. The Application Code to be checked for Vulnerability Assessment (VA) carried out and for other Security requirements iii. The Application Code to be tested against at least OWASP Top 10 vulnerabilities. iv. The Application Code to be checked for the database connection and database queries. v. Perform Vulnerability Assessment (VA) on current Application and Application running at the time of incident in H2 of CY 2024, both in staging environment. vi. Report pertaining to application code review. <p>c) Backup Review</p> <ul style="list-style-type: none"> i. Study of the backup and retention policy / procedure of BHEL as well as regulatory instructions applicable to the Application under review. ii. Application Code and Database backup and retention review. Any deviation from best practice or Company policies / regulatory instructions to be brought out. iii. Report pertaining to application code review. <p>d) Server (Application / Hardware) Review</p> <ul style="list-style-type: none"> i. Report on Application server configuration. ii. Report on the various types of server logs configured, generated and their 		
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

Ref. No. AA: CDT: ACS:CPS-Audit dtd. 20.09.2025

To be signed and stamped by the bidder

Page 4

	<p>relevance and sufficiency including such logs that were required or desirable but were not provided.</p> <p>iii. Report on the Server OS hardening done and any other hardening measure required to be done.</p> <p>iv. Any loopholes as per the best practice to be brought out & covered in the aforementioned reports in d (i), d(ii) and d(iii).</p> <p>e) Business Continuity Plan Review</p> <p>i. Report on Operational procedures of Application server and database server.</p> <p>ii. Report on the existence and testing of the Business Continuity Plan of the Application.</p>		
M2	<p>a. Incident Report</p> <p>i. A detailed Incident Report to be submitted detailing the chronology of events, credentials used, vulnerability exploited, root cause, users involved etc.</p> <p>ii. Corrective actions to be taken for the Application, database, backup, application testing, server hardening, application logs etc. to be also included in the report.</p> <p>iii. Preventive actions to be taken so that such incidents in this Application and similar incidents do not recur to be included in the report.</p>		

NOTE: A Deliverable / Report should be compliant to specifications, contract and in the manner accepted by BHEL

2.0 Table 2: Milestones, Deliverables & Delivery Timelines

Milestone	Deliverables	Timelines Start	Timelines End
M1	a. Application Development / Implementation Review b. Application Code Review c. Backup Review d. Server (Application / Operating System (OS) Review e. Business Continuity Plan Review	D*	D + 60 Days
M2	a. Incident Report	D*	D +75 Days
* : D-Date of award of WO /PO - Start Date			

Post-Report Support:

Post Submission of the incident report CDAC shall, support BHEL in reviewing stakeholder submissions related to identified queries, deviations, and red flags, as cited in their report and shall advise on the requirement for any further clarification or consequential measures

- 3. Location:** The Access to the resources/servers/data may be made available from BHEL Hyderabad location, However, if any physical visit to the server physical location or at the location of the incident [Delhi/Haridwar] will be required, BHEL will arrange for the Boarding and Lodging at BHEL guest house for the vendor team.

4. Review & monitoring:

Periodic review shall be held preferably on a fortnightly basis or at such intervals as may be desired by BHEL, in consultation with CDAC. The timing, agenda, and conduct of such reviews shall be as decided by BHEL, in consultation with CDAC with the purpose of monitoring progress, resolving issues, and ensuring adherence to deliverables and timelines.

5. Settlement of Disputes:

In case of Contract with Public Sector Enterprise (PSE) or a Government Department, the following shall be applicable:

In the event of any dispute or difference relating to the interpretation and application of the provisions of commercial contract(s) between Central Public Sector Enterprises (CPSEs)/ Port Trusts inter se and also between CPSEs and Government Departments/Organizations (excluding disputes concerning Railways, Income Tax, Customs & Excise Departments), such dispute or difference shall be taken up by either party for resolution through AMRCD (Administrative Mechanism for Resolution of CPSEs

Ref. No. AA: CDT: ACS:CPS-Audit dtd. 20.09.2025

To be signed and stamped by the bidder

Disputes) as mentioned in DPE OM No. 05/0003/2019-FTS-10937 dated 14-12-2022 as amended from time to time.

6. SD/EMD/Penalty for Late Delivery

Not applicable

7. PQR

Not applicable

8. Taxes & Duties :

As Applicable

9. Service Level Agreement (SLA):Not applicable

10. Bonus Clauses, PVC, ORC, Risk Purchase: Not applicable

11. Payment Terms:

- i. 40% payment will be released within 15 days of placement of PO against Proforma Invoice.
- ii. Balance payments 60% will be released within 30 days after receipt of Tax Invoices on completion of milestone M2 :

12. Location & Consignee Address

Name: Kamal Sharma
Designation: Sr. Manager (CDT)
2nd Floor, HRDI Building
BHEL HRDI & ESI Complex, Plot No-25
Sector -16 A, Film city
Noida, U.P. - 201301
Contact details: 0120-2416490
Email: kamal.sharma@bhel.in

13. Non-Disclosure Agreement:

All the material / information sent to the bidder shall be treated as confidential and should not be disclosed in any matter to any unauthorized person under any circumstances. The bidder has to furnish a Non- Disclosure Agreement (NDA) (as per Annexure-I) in line with the Owner's Information Security Management System (ISMS).

14. Laws Governing the Contract:

The order/ contract shall be executed and governed by the laws of India and the courts of India alone shall have jurisdiction in respect of any matter arising under or in connection with the order/ contract. Courts at Delhi/ New Delhi shall have exclusive jurisdiction to decide the dispute, if any, arising out of or in respect of the contract to which these conditions are applicable.

15. Force Majeure:

Vendor shall not be responsible for delay in delivery resulting from acts / events beyond his control, provided notice of the happening of any such act / event is given by the Vendor to the Purchaser within

Ref. No. AA: CDT: ACS:CPS-Audit dtd. 20.09.2025

To be signed and stamped by the bidder

Page 7

15 days from the date of its occurrence. Such acts / events shall include but not be limited to acts of God, war, floods, earthquakes, strikes, lockouts, epidemics, riots, fire or Governmental regulations superimposed after the date of order / contract.

16. Bid Documents

Bid shall be accepted by the official inviting the tender in **ONE PART**.

Bid shall consist of the following:

- i) PRICE BID as per as per format enclosed as **S.No 17**
- ii) Third party non- disclosure agreement (NDA) format enclosed as **Annexure-I**

Price bid containing PRICES only is to be submitted as per Price Bid Format. Prices shall be quoted in Indian Rupees only.

17. Price Bid Format

S.NO	Activity	Charges in INR (excl of Taxes)
01	Security Audit as per Scope of Work	
Cost in words [INR]		
Applicable GST rate [%]		
GST Amount [INR]		
Total charges inclusive of GST [INR]		

Annexure- I

MUTUAL NON-DISCLOSURE AGREEMENT

This Agreement is made and entered into as of the last date signed below (the "Effective Date") by and between **Bharat Heavy Electricals Ltd.(BHEL)**, a Public Sector Organization having its principal place of business at BHEL House, Siri Fort, New Delhi - 110049 and _____, a _____ corporation, hereinafter called "The Bidder", whose principal mailing address is _____.

WHEREAS in order to pursue the mutual business purpose of this particular project as specified in Bid document for Security Audit as per Scope of Work, **BHEL** and the Bidder have an interest in participating in discussions wherein either Party might share information with the other that the disclosing Party considers to be proprietary and confidential to itself ("Confidential Information"); and

WHEREAS the Parties agree that Confidential Information of a Party might include, but not be limited to that Party's:

1. business plans, methods, and practices;
2. personnel, customers, and suppliers;
3. inventions, processes, methods, products, patent applications, and other proprietary rights; or
4. specifications, drawings, sketches, models, samples, tools, computer programs, technical information, or other related information;

NOW, THEREFORE, the Parties agree as follows:

1. Either Party may disclose Confidential Information to the other Party in confidence provided that the disclosing Party identifies such information as proprietary and confidential either by marking it, in the case of written materials, or, in the case of information that is disclosed orally or written materials that are not marked, by notifying the other Party of the proprietary and confidential nature of the information, such notification to be done orally, by e-mail or written correspondence, or via other means of communication as might be appropriate.
2. When informed of the proprietary and confidential nature of Confidential Information that has been disclosed by the other Party, the receiving Party ("Recipient") shall, for a period of three (3) years from the date of disclosure, refrain from disclosing such Confidential Information to any contractor or other third party without prior, written approval from the disclosing Party and shall protect such Confidential Information from inadvertent disclosure to a third party using the same care and diligence that the Recipient uses to protect its own proprietary and confidential information, but in no case less than reasonable care. The Recipient shall ensure that each of its employees, officers, directors, or agents who has access to Confidential Information disclosed under this Agreement is informed of its proprietary and confidential nature and is required to abide by the terms of this Agreement. The Recipient of Confidential Information disclosed under this Agreement shall

Ref. No. AA: CDT: ACS:CPS-Audit dtd. 20.09.2025

To be signed and stamped by the bidder

Page 9

promptly notify the disclosing Party of any disclosure of such Confidential Information in violation of this Agreement or of any subpoena or other legal process requiring production or disclosure of said Confidential Information.

3. All Confidential Information disclosed under this Agreement shall be and remain the property of the disclosing Party and nothing contained in this Agreement shall be construed as granting or conferring any rights to such Confidential Information on the other Party. The Recipient shall honor any request from the disclosing Party to promptly return or destroy all copies of Confidential Information disclosed under this Agreement and all notes related to such Confidential Information. The Parties agree that the disclosing Party will suffer irreparable injury if its Confidential Information is made public, released to a third party, or otherwise disclosed in breach of this Agreement and that the disclosing Party shall be entitled to obtain injunctive relief against a threatened breach or continuation of any such breach and, in the event of such breach, an award of actual and exemplary damages from any court of competent jurisdiction.
4. The terms of this Agreement shall not be construed to limit either Party's right to develop independently or acquire products without use of the other Party's Confidential Information. The disclosing party acknowledges that the Recipient may currently or in the future be developing information internally, or receiving information from other parties, that is similar to the Confidential Information. Nothing in this Agreement will prohibit the Recipient from developing or having developed for it products, concepts, systems or techniques that are similar to or compete with the products, concepts, systems or techniques contemplated by or embodied in the Confidential Information provided that the Recipient does not violate any of its obligations under this Agreement in connection with such development.
5. Notwithstanding the above, the Parties agree that information shall not be deemed Confidential Information and the Recipient shall have no obligation to hold in confidence such information, where such information:
 - 5.1. Is already known to the Recipient, having been disclosed to the Recipient by a third party without such third party having an obligation of confidentiality to the disclosing Party; or
 - 5.2. Is or becomes publicly known through no wrongful act of the Recipient, its employees, officers, directors, or agents; or
 - 5.3. Is independently developed by the Recipient without reference to any Confidential Information disclosed hereunder; or
 - 5.4. Is approved for release (and only to the extent so approved) by the disclosing Party; or
 - 5.5. Is disclosed pursuant to the lawful requirement of a court or governmental agency or where required by operation of law.
6. Nothing in this Agreement shall be construed to constitute an agency, partnership, joint venture, or other similar relationship between the Parties.
7. Neither Party will, without prior approval of the other Party, make any public announcement of or otherwise disclose the existence or the terms of this Agreement.

Ref. No. AA: CDT: ACS:CPS-Audit dtd. 20.09.2025

To be signed and stamped by the bidder

Page 10

8. This Agreement contains the entire agreement between the Parties and in no way creates an obligation for either Party to disclose information to the other Party or to enter into any other agreement.
9. Deletion of any data remained after the scope of the work has been completed.
10. This Agreement shall remain in effect during the contract period from the Effective Date unless otherwise terminated by either Party giving notice to the other of its desire to terminate this Agreement. The requirement to protect Confidential Information disclosed under this Agreement shall survive termination of this Agreement.

IN WITNESS WHEREOF:

FOR AND ON BEHALF OF

FOR AND ON BEHALF OF

BHARAT HEAVY ELECTRICALS LTD.

Signature: _____

Signature: _____

Name: _____

Name: _____

Designation: _____

Designation: _____

Date: _____

Date: _____

Witness

Witness

1.

1.

2.

2.

Ref. No. AA: CDT: ACS:CPS-Audit dtd. 20.09.2025

To be signed and stamped by the bidder

Page 11