

GOVERNMENT OF INDIA
MINISTRY OF HEAVY INDUSTRIES
LOK SABHA
UNSTARRED QUESTION NO. 452
ANSWERED ON 21.07.2026

**CYBERSECURITY VULNERABILITIES IN E-RICKSHAW BMS AND ROLE OF
CERTIFICATION AGENCIES**

**452. SHRI SURESH KUMAR SHETKAR:
SHRI VIJAYAKUMAR ALIAS VIJAY VASANTH:
SHRI MANICKAM TAGORE B:**

Will the Minister of HEAVY INDUSTRIES be pleased to state:

- (a) whether it has taken note of incidents where e-rickshaw batteries were remotely disabled through mobile applications, leading to public inconvenience and extortion, if so, details thereof;
- (b) whether the Government has identified security vulnerabilities in battery management systems (BMS) used in electric vehicles, particularly those controlled through foreign-developed applications, if so, findings thereof;
- (c) whether the Government has issued any advisories to manufacturers and operators regarding use of insecure battery management applications, if so, details thereof;
- (d) whether the Government state whether certification agencies such as ARAI and ICAT currently mandate cybersecurity standards while approving electric vehicles and battery systems, if so, details thereof, if not, the reasons therefor;
- (e) whether the Government has taken cognisance of reports that existing certification norms focus only on mechanical and electrical safety without addressing cybersecurity risks, if so, the details thereof; and
- (f) whether the Government clarify as any guidelines exist for prevent unauthorised remote access or shutdown of electric vehicle batteries, if so, details thereof and if not, reasons for regulatory gap?

**ANSWER
THE MINISTER OF STATE FOR HEAVY INDUSTRIES
(SHRI BHUPATHIRAJU SRINIVASA VARMA)**

(a) & (b): The Indian Computer Emergency Response Team (CERT-In) has received reports of safety concern involving electric three-wheelers (e-rickshaws). It has been reported that it is possible for unauthorized individuals to abruptly power off moving e-rickshaws by using a publicly available BMS mobile application. The issue lies in the Bluetooth module of the Battery Management System (BMS) chip, which is embedded in the battery module. The BMS commonly found in the low-cost e-rickshaws, have default or no credentials, which allows unauthorised users to connect and modify the settings and/or cut off the battery's discharge, causing sudden vehicle shutdowns. CERT-In has identified the mobile apps which can be used to abruptly power-off batteries of erickshaws and reported to MeitY to remove the apps from application play stores.

(c): MHI has issued advisory for addressing Bluetooth BMS vulnerabilities in e-rickshaws to SIAM, ACMA Industry bodies and testing agencies.

(d) to (f): As per the information received from Ministry of Road Transport and Highways(MoRTH) cybersecurity regulations have not been framed in respect of E-rickshaw and E-kart. However, the Battery Safety Requirements for L-category EVs shall meet the standards prescribed in AIS 156 and Electric Power Train Safety shall comply with AIS 038 Rev. (2). The Government in the Ministry of Road Transport and Highways vide G.S.R. 503(E) dated 17th June, 2026 has published draft rules for approval of vehicles about cyber security in respect of vehicles of category L, M and N as per AIS- 189 and AIS- 190. Further, Rule 126 of the CMVR, 1989 mandates that every manufacturer or importer of a motor vehicle, including electric vehicles, shall submit the prototype to a testing agency notified under Rule 126. The testing agency issues a Type Approval Certificate certifying compliance with the provisions of the Motor Vehicles Act, 1988 and the CMVR, 1989.
