

**GOVERNMENT OF INDIA
MINISTRY OF ROAD TRANSPORT AND HIGHWAYS**

**LOK SABHA
UNSTARRED QUESTION NO. - 808
ANSWERED ON 23rd JULY, 2026**

CYBERSECURITY OF ADVANCED TECHNOLOGY VEHICLES

808. SHRI G M HARISH BALAYOGI:

Will the Minister of ROAD TRANSPORT AND HIGHWAYS

सड़क परिवहन और राजमार्ग मंत्री

be pleased to state:

- (a) the details regarding cyberattacks, malware, unauthorised access and other cybersecurity incidents involving vehicles and vehicle software systems reported across the country;**
- (b) the details of the existing regulatory framework governing cybersecurity and software update management in technologically advanced vehicles, including the categories of vehicles covered and the standards prescribed;**
- (c) whether any gaps have been identified in the existing framework for securing vehicle software systems, including battery management systems against cyber threats and if so, the steps taken or proposed to be taken to address the same;**
- (d) the mechanism for testing, certification, monitoring and enforcement of vehicle cybersecurity and software update systems and the agencies responsible for the same; and**
- (e) the steps taken or proposed to align India's vehicle cybersecurity standards with applicable international regulations and to strengthen**

cybersecurity and software update management in connected and advanced technology vehicles?

ANSWER

THE MINISTER OF ROAD TRANSPORT AND HIGHWAYS

(SHRI NITIN JAIRAM GADKARI)

(a) 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.

CERT-In has identified the mobile apps which can be used to abruptly power-off batteries of e-rickshaws and reported to MeitY to remove the apps from application play stores.

(b) 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 cyber security in respect of vehicles of category L, M and N as per AIS-189 and AIS- 190 inviting comments and objections.

(c) and (e) With a view to harmonising the national standards with the internationally accepted regulatory framework, the provisions of UN Regulation No. 155 on Cybersecurity and Cybersecurity Management Systems (CSMS) and UN Regulation No. 156 on Software Update and Software Update Management Systems (SUMS) were transposed and AIS-189, titled Approval of Vehicles with regard to Cybersecurity and Cybersecurity Management System (CSMS), and AIS-190, titled Approval of Vehicles with regard to Software Update and Software Update Management System (SUMS), were formulated to establish the technical and procedural requirements for the approval of motor

vehicles concerning cybersecurity and over-the-air (OTA) software updates.

(d) Rule 126 of the Central Motor Vehicle Rules (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.
