

GOVERNMENT OF INDIA  
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY  
**LOK SABHA**  
**UNSTARRED QUESTION NO. 657**  
TO BE ANSWERED ON: 22.07.2026

**MISUSE OF MOBILE APPLICATIONS TO REMOTELY DISABLE E-RICKSHAWS**

†657. **SHRI CHANDAN CHAUHAN:**

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

- (a) whether the Government has taken cognizance of the instances of misuse of mobile applications associated with battery management systems to remotely disable e-rickshaws and other electric vehicles and extort money from drivers particularly economically weaker e-rickshaw drivers, on the pretext of restoring the vehicles to operational condition;
- (b) if so, whether the Government, in coordination with the State Governments, proposes to identify the individuals and entities responsible for such incidents, initiate penal action against them and provide appropriate relief to the affected drivers;
- (c) if so, whether the Government proposes to implement mandatory cyber security and authentication standards for mobile applications and battery management systems associated with electric vehicles; and
- (d) the details of other measures being taken by the Government to prevent the recurrence of such incidents and to ensure consumer protection in view of the increasing use of electric vehicles in the country?

**ANSWER**

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY  
(SHRI JITIN PRASADA)

(a) to (d): Government has taken cognizance of reports regarding the misuse of certain Battery Management System (BMS) mobile applications that enabled unauthorised remote control of e-rickshaw batteries. On 3<sup>rd</sup> July 2026, Government issued orders for removal of such applications on app stores.

Further, Government has institutionalised a nationwide integrated and coordinated framework to strengthen cybersecurity and digital resilience across digital ecosystems, which, inter alia, includes:

- i. National Cyber Security Coordinator (NCSC) under the National Security Council Secretariat (NSCS) to ensure coordination related to cyber security amongst different agencies.
- ii. The Indian Computer Emergency Response Team (CERT-In) is designated as the national agency for responding to cyber security incidents under the provisions of section 70B of the Information Technology (IT) Act, 2000.
- iii. National Cyber Coordination Centre (NCCC), implemented by CERT-In, examines the cyberspace to detect cyber security threats. It shares the information with concerned organizations, state governments and stakeholder agencies for taking action.
- iv. The Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country under the provisions of section 70A of the IT Act, 2000.
- v. The Consumer Protection Act, 2019, administered by the Department of Consumer Affairs, Ministry of Consumer Affairs, Food and Public Distribution, was enacted to modernize the

framework governing consumer protection in the era of globalization, technologies, e-commerce markets, etc.

- vi. 'Information Security Education and Awareness (ISEA)' project is implemented by MeitY for strengthening human resources in the area of Information Security and creating general awareness. Awareness material on various aspects of cyber hygiene & cyber security is disseminated through portals such as [www.staysafeonline.in](http://www.staysafeonline.in), [www.infosecawareness.in](http://www.infosecawareness.in) and [www.csk.gov.in](http://www.csk.gov.in).

\*\*\*\*\*