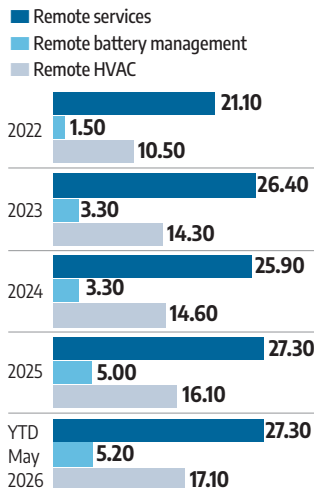


Centre asks OEMs to audit connected vehicles' software



Shifting gears

Connected car penetration in India (%)



HVAC: Heating, ventilation, and air conditioning
Source: JATO Dynamics

AASHISH ARYAN & SHINE JACOB

New Delhi/Chennai, 7 July

The Central government has asked automobile and parts makers to thoroughly audit the software and devices that control connected cars and electric vehicles (EVs) including commercial vehicles, two persons aware of the development told *Business Standard*.

The government's communication to the auto industry in the form of an advisory, however, stops short of specifying a deadline for conducting the audit, said the persons who spoke on condition of anonymity.

This comes after the government directed Apple and Google last week to take down three apps over EV hacking concerns.

In a letter to the Society of Indian Automobile Manufacturers (Siam) and the Automotive Component Manufacturers Association of India (Acma) this week, the Ministry of Heavy Industries has urged companies to audit their battery communication interfaces and eliminate unsecured default settings, weak authentication, or unprotected over-the-air pathways, the persons said.

The ministry did not respond to *Business Standard's* queries till

the time of publishing.

The heavy industries ministry also told automakers to work with other ministries handling road transport and highways and electronics and information technology as well as other stakeholders for better, more resilient cyber safety design protocols at the factory level.

The letter called the hacking incidents a critical security vulnerability that requires immediate attention and coordinated action across the automotive sector. One of the persons quoted above said the main security concern before the government was regarding connected cars.

The government last week banned three apps that were being misused to arbitrarily stop EVs such as e-autorickshaws and two-wheelers after taking unauthorised control of the battery management devices installed in these vehicles.

The three apps, BAT-BMS, Lossigy, and Epoch-ion, were removed from both the App Store and the Play Store after videos surfaced on social media showing these apps being misused to remotely disable EVs. These apps are used for monitoring battery levels, temperature, and cycle life in EVs.

Turn to Page 7 ▶

Centre asks OEMs to audit connected vehicles' software

They allow users to connect to the battery management device fitted inside EVs via Bluetooth. Early this year, a draft notification by the road transport and highways ministry proposed a phased rollout of certain standards for connected vehicles starting October 1, 2026.

"Manufacturers must begin building systematic cyber security management systems and software update management systems now," the letter stated.

"This includes securing over-the-air (OTA) updates, implementing robust user authentication, and validating software integrity," it added.

According to data from

automotive intelligence firm JATO Dynamics, various connected car features have increased in the last few years.

Of these, remote services (app-based remote access and control functions) increased from 21 per cent in 2022 to 27 per cent in 2026, while remote battery management was up from 1.5 per cent to 5.2 per cent during the same period. Similarly, remote heating, ventilation and air conditioning also increased from 10.5 per cent to 17.1 per cent during the period, shows JATO Dynamics' data.

Though BAT-BMS (developed by Shenzhen Grenergy Technology) is a legitimate tool designed to manage Bluetooth-enabled battery systems, the government has indicated that a serious security loophole opens up when low-cost lithium battery packs are deployed with default factory settings, weak passwords, or no Bluetooth authentication.

Because of this, anyone can stand within 10 to 15 metres to connect to the vehicle via the app and cut off the "Dis-

charge" function. The motor instantly loses power, and the vehicle grinds to a halt mid-transit. The government believes that removing the apps only addresses the symptom. The underlying vulnerability in these communication interfaces remains unaddressed.

"Unlike smartphones, there is no dominant operating system for connected vehicles. There is no common connected vehicle software platform across the Indian

automotive industry. Most manufacturers operate proprietary connected vehicle ecosystems developed either in-house or with technology partners," said Ravi Bhatia, presi-

dent, JATO Dynamics.

Consumer-facing services include Suzuki Connect (Maruti Suzuki), Hyundai Bluelink, Kia Connect, Tata iRA (Intelligent Real-time Assist), Mahindra AdrenoX Connect, MG i-SMART, and Honda Connect. The underlying software is typically developed with global automotive technology suppliers such as Bosch, Harman, Continental, Qualcomm, and Tata Technologies/KPIT Technologies, while cloud infrastructure is commonly provided by Amazon Web Services (AWS), Microsoft Azure, or Google Cloud.

While recent safety updates have successfully integrated telematics and connected features into modern battery architectures, these standards do not mandate specific wireless technologies, nor do they guarantee absolute immunity from cyber threats, the letter added.

According to Bhatia, vehicle data is typically transmitted from the vehicle's Telematics Control Unit (TCU) to

the OEM's cloud platform over a secure cellular connection.

Most manufacturers use hyperscale cloud providers such as Amazon Web Services, Microsoft Azure, or Google Cloud to store and process the data. Storage location depends on each manufacturer's global IT architecture and regulatory requirements. Increasingly, data relating to Indian customers is stored or mirrored in India to meet evolving data residency and privacy requirements. Concerns regarding

software and technology sources are not isolated with regard to connected vehicles, said Sunil Dahiya, founder and lead analyst at Envirocatalysts, a policy think tank. Several other sectors, like power, are even more susceptible to hacking and such cyberattacks, said Dahiya.

"While it is true that there should be an audit and a legal framework to monitor them, the moves should not affect the pace of growth of autonomous technologies," said Dahiya.

SBI joins global banks to fund Sun's \$11.75 bn deal

In recent times, there has been a resurgence of outbound acquisitions by Indian corporates. According to experts, some of the factors driving the trend are access to technology in a rapidly evolving manufacturing and industrial landscape, and the restructuring of global supply chains, with near-shoring and on-shoring now a structural rather than cyclical trend.

Moreover, as some Indian companies face muted domestic growth, they are looking outward to sustain their historical pace of expansion — backed by robust balance sheets that some bankers believe are 'perhaps in their best ever' health. Sectors

seeing active outbound interest include pharmaceuticals, health care, electronic manufacturing services (EMS), and information technology (IT).

"Many of these acquisitions provide Indian companies with access to overseas markets, technology or customers. The manufacturing activity often remains in India or is brought back to India after the acquisition. Companies may acquire technology, customer access or established brands, all of which eventually support domestic investment", PD Singh, Standard Chartered Bank's India and South Asia chief executive officer told *Business Standard* recently.

QIPs rebound as market sentiment revives

The latter followed a framework agreement between the US and Iran aimed at easing regional tensions. QIP, being an easily executable fundraising option, has aided this strong rebound.

And, unlike initial public offerings, QIPs are done in listed companies with a strong public record of their business model and valuations, making it easier for investors to take a call.

"The revival in QIPs during the second half of June was driven by a broader improvement in market sentiment," said Ambareesh

Baliga, an independent equity analyst.

"Unlike the earlier rally, this one saw much wider participation across the market, giving management teams greater confidence in valuations. While liquidity had been available throughout, companies also needed to be comfortable with the prices at which they were raising capital," said Baliga.

Since the beginning of the financial year, the Nifty has gained 9.3 per cent, the Nifty Midcap 100 has risen 18.3 per cent, and the Nifty Smallcap