GOVERNMENT OF INDIA
MINISTRY OF COMMUNICATIONS
DEPARTMENT OF TELECOMMUNICATIONS

LOK SABHA
UNSTARRED QUESTION NO. 2910
ANSWERED ON 6TH AUGUST, 2025

NATIONAL CYBER SECURITY COORDINATOR

2910. MS SAYANI GHOSH:

Will the Minister of COMMUNICATION be pleased to state:

(a) whether the Government is aware of recent findings by the National Cyber Security Coordinator (NCSC) regarding the presence of chipsets of Chinese origin in certain mobile SIM cards and if so, the number of such cases identified and the telecom operators or vendors involved;

(b) whether the Government is considering a nationwide replacement of older SIM cards due to potential national security risks and if so, the details thereof;

(c) whether the Government has identified the techno-legal and financial implications of such a replacement exercise for telecom operators and consumers and if so, the details thereof;

(d) the steps taken by the Government to strengthen the trusted sourcing and continuous auditing of telecom components including SIM cards, to prevent unauthorised or unapproved imports; and,

(e) whether the Government is considering utilising the eSIM (embedded SIM) in order to avoid cybersecurity threats and reliance on Chinese imports and if so, the details thereof?

ANSWER

MINISTER OF STATE FOR COMMUNICATIONS AND RURAL DEVELOPMENT
(DR. PEMMASANI CHANDRA SEKHAR)

(a) It has been informed by NSCS that the issue raised in question mentioning “National Cyber Security Coordinator" pertains to the implementation of the National Security Directive for Telecom Sector (NSDTS) issued by NSCS is implemented based on evaluations from security agencies by the National Security Committee on Telecom (NSCT) chaired by Deputy NSA. The inputs, deliberations and the basis for the conclusions are classified as secret and have national security implications.

(b) Currently, no nationwide replacement of older SIM cards is being considered.

(c) In view of reply to part (b), the question does not arise.

(d) Steps taken by the Government to strengthen trusted sourcing and continuous auditing of telecom components to prevent unauthorized or unapproved imports are as follows:

i. The **National Security Directive on Telecommunication Sector (NSDTS)** was **approved by the Union Cabinet on December 16, 2020.** It mandates that all the **Telecommunication entities** in India must **procure and deploy only "trusted products" sourced from "trusted vendors"** to safeguard national security. The Department of Telecommunications launched the **Trusted Telecom Portal** (trustedtelecom.gov.in) to facilitate compliance.

ii. The Government has amended various License Agreements, including the Unified License (UL), UL (VNO), Unified Access Service License, and Standalone Licenses, to incorporate a specific condition related to the procurement and installation of Telecommunication Equipment by licensees in their networks. This condition mandates that, with effect from **15.06.2021**, licensees are permitted to connect only *Trusted Products*—as notified by the *Designated Authority* (i.e., the National Cyber Security Coordinator) on the **Trusted Telecom Portal**—in their networks. Licensees must also obtain prior permission from the Designated Authority for any upgradation or expansion of existing networks using Telecommunication Equipment not designated as Trusted Products. Further, to ensure compliance with the above provisions, all licensees are required to submit a **half-yearly compliance report** through the **Saral Sanchar Portal** on **1st January** and **1st July** of each year. In addition, **audits of telecom entities are conducted by the Licensed Service Area (LSA) field units of the Department of Telecommunications (DoT)** to ensure adherence to the prescribed guidelines.

iii. The Department of Telecommunications (DoT) has issued Indian Telecommunication Security Assurance Requirements (ITSAR)—a set of baseline security requirements for telecom equipment to ensure a secure and trusted communication infrastructure—which cover all Pluggable (U)ICC, including SIM, USIM, and other (U)ICC-based applications/applets. Additionally, SIM cards are covered under the Mandatory Testing and Certification of Telecom Equipment (MTCTE)—a scheme that mandates telecom equipment be tested and certified to ensure compliance with Indian technical standards. Furthermore, in 2021, DoT has also issued a Standard Operating Procedure (SOP) specifically for SIM personalization to ensure trusted sourcing and continuous auditing of telecom components.

(e) The Department of Telecommunications (DoT) has released Indian Telecommunication Security Assurance Requirements (ITSAR) for eSIM, and it is also covered under the Mandatory Testing and Certification of Telecom Equipment (MTCTE). The SOP for eSIM personalization is currently under process.

*****