GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

RAJYA SABHA

UNSTARRED QUESTION NO. 870

TO BE ANSWERED ON: 06.02.2026

USE OF FOREIGN AI PLATFORMS BY GOVERNMENT OFFICIALS

870. SHRI MALLIKARJUN KHARGE:

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

(a) whether Government has assessed the risks arising from the use of foreign Artificial Intelligence (AI) platforms by Government officials for official tasks such as document summarisation or policy drafting;
(b) whether any instances of sensitive or internal Government data being exposed to such platforms have been identified, if so, the number of cases reported during the last five years; and
(c) whether Government proposes to issue guidelines or restrictions governing the use of generative AI tools by public servants?

ANSWER

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

(a) to (c): India's AI strategy is based on the Hon'ble Prime Minister's vision of democratizing technology. It aims to address India centric challenges and create opportunities.

The Government is aware of the risks associated with the use of generative AI by government officials. Government officials using any AI tools or IT products are subject to the provisions of Official Secrets Act.

Indian Computer Emergency Response Team (CERT-In) has issued guidelines issued by that provide specific safeguards for the safe and responsible use of AI tools:

- An advisory on safety measures to be taken to minimize the adversarial threats arising from Artificial Intelligence (AI) based applications was published in May 2023.
- The Certified Security Professional in Artificial Intelligence (CSPAI) program launched by CERT-In and SISA in September 2024.
- An advisory depicting best practices for effective and responsible use of Generative AI solutions was published in March 2025.
- The CSPAI program equips cybersecurity professionals with the skills to secure AI systems, proactively address AI-related threats, and ensure trustworthy AI deployment in business environments.
- CERT-In has issued guidelines on information security practices for government entities in June 2023 covering domains such as data security, network security, identity and access management, application security, third-party outsourcing, hardening procedures, security monitoring, incident management and security auditing.
- Cyber security mock drills by CERT-In for assessment of cyber security posture and preparedness of organisations in Government and critical sectors.
- Cyber security training programs conducted by CERT-In in collaboration with Industry partners to upskill the cyber security workforce in Government, public and private organizations. 23 and 32 training programs were conducted covering 12014 and 20799 participants during 2024 and 2025 respectively.

- CERT-In co-signed ANSSI’s February 2025 report “Building trust in AI through a cyberrisk-based approach” advocating a risk-based framework to secure AI systems and value chains and urging global dialogue on mitigating AI-related cyber risks for trusted development.

*****