GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 706
TO BE ANSWERED ON: 05.12.2025

THREAT OF DATA LEAK DUE TO RISING USE OF AI PLATFORMS BY GOVERNMENT OFFICIALS

706. SHRI S NIRANJAN REDDY:

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

(a) whether Government is aware that generative AI platforms may extract sensitive information from prompts input by government officials using such tools for note-making, analysis, or administrative assistance;
(b) whether any assessment has been conducted on the risk of AI systems storing, profiling or learning from inputs related to Government policies;
(c) whether guidelines have been issued or are proposed, to regulate the use of commercial AI tools by civil servants;
(d) whether Government proposes to establish secured sovereign AI models or in-house large language models (LLMs) for official use; and
(e) if so, the details thereof, and if not, the reasons therefor?

ANSWER

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

(a) to (e): 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 and are not supposed to share any classified or sensitive information on platforms that are not secure or hosted outside of India.

Hosting of Open-Source Models: To promote secure access to AI tools, MeitY has enabled hosting of open-source AI models on the AIRAWAT compute infrastructure managed by C-DAC Pune. This obliviates the risk of transfer of sensitive data out of the country. Models from the LLAMA, OpenAI and Mistral families have been deployed. These are also being made available to developers through APIs on a chargeable basis.

Further, NIC is providing access to open-source models installed on premises through the Meghraj cloud of NIC for Government users.

Under the AIKosh platform, 251 AI models and more than 27 development toolkits specific to India are also made available.

India's own Foundational Models under the IndiaAI Mission: Government launched IndiaAI mission in March 2024. The IndiaAI Foundation Models pillar aims to develop India's own large multimodal models trained on Indian datasets and languages to ensure sovereign capability and global competitiveness in generative AI.

Twelve organisations and consortia, including startups, industry players and academic institutions, including Sarvam AI, Soket AI, Gnani AI, Gan AI, Avatar AI, IIT Bombay Consortium (BharatGen), GenLoop, Zentieq, Intellihealth, Shodh AI, Fractal Analytics Ltd. and Tech Mahindra Maker's Lab, have been selected for developing Large and Small Language Models based on Indian datasets.

The resulting AI models will contribute to the open-source ecosystem and be available for use by Government organizations and also support innovation across India's startup and research community.

Indian Computer Emergency Response Team (CERT-In): The guidelines issued by the Indian Computer Emergency Response Team (CERT-In) 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 co-signed ANSSI's February 2025 report "Building trust in AI through a cyber-risk-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.

*****