

GOVERNMENT OF INDIA  
MINISTRY OF AGRICULTURE AND FARMERS WELFARE  
DEPARTMENT OF AGRICULTURAL RESEARCH & EDUCATION

**RAJYA SABHA**  
**UNSTARRED QUESTION NO-1450**  
ANSWERED ON- 12/12/2025

**ICAR DATA BREACH**

1450. SMT. JEBI MATHER HISHAM:

Will the Minister of AGRICULTURE AND FARMERS WELFARE be pleased to state:

- (a) whether Government has assessed the reasons for March-April 2025 ICAR data breach that compromised recruitment data, research projects, financial records and internal communications, if so, the details thereof;
- (b) immediate steps taken to restore systems at New Delhi Data Centre and the NAARM-Hyderabad replication server;
- (c) ICAR Research Institutes affected by the breach;
- (d) the key finding of the High-Level Committee and whether any criminal case has been registered, and if so, its present status;
- (e) whether accountability has been fixed on the officials responsible, details thereof;
- (f) whether CERT has initiated its inquiry, details thereof; and
- (g) concrete measures introduced to prevent such breaches in future?

**ANSWER**

THE MINISTER OF STATE FOR AGRICULTURE AND FARMERS WELFARE  
(SHRI BHAGIRATH CHOUDHARY)

(a): Yes. ICAR Data Centre was attacked through a Ransomware. It was found out to be a variant of Lockbit Ransomware.

(b):

- The incident was reported to CERT-In on April 01, 2025 (Case id: CERT-In-32082725).
- It was reported to Cyber Crime Reporting Portal on April 04, 2025 (Acknowledgement No. 20804250024658).

- The necessary steps were taken for restoration as per the CERT-In recommendations.
- Apart from this, various relevant agencies of Govt. of India were contacted for restoration of this system. The teams from following agencies visited the Data Centre for the same:
  - CERT-In Team
  - Indian Cybercrime Coordination Centre (I4C)
  - National Investigation Agency (NIA)
  - Cyber Multi Agency Centre (CyMAC)
  - IB under MHA
  - C-DAC Trivandrum.

(c): Total 88 ICAR Institutes websites were affected out of which 71 are restored.

(d): The key observations of the High-Level Committee were related to:

- Strengthening cyber security framework of the Data Centre.
- Improving institutional capability to manage cyber security emergencies.
- Upgrading infrastructure and software with latest globally available technologies.
- Implementation of strong backup policies and Data Recovery protocols.
- Establishment of protocol for early verification of data theft and damage control.
- Improve ICT related communication and coordination within ICAR.
- Identification of gaps in coordination and fixing responsibility.
- Extensive training of officers and staff for monitoring and management of Cyber Security of Data Centre.

The incident was reported on April 01, 2025 to CERT-In (Case id: 32082725) and complaint on National Cyber Crime Reporting Portal on April 04, 2025 (Acknowledgement No. 20804250024658). Subsequently, the complaint has been assigned to Cyber Police Station (West), Delhi on April 09, 2025.

(e): Three committees for fixing accountability have been constituted vide Order dated 1.10.2025, 24.10.2025 and 10.11.2025 at ICAR Hqrs.

(f): Yes. Restoration is being done as per CERT-In recommendation.

(g): A research data management policy has been made and circulated to all Institutes for adherence. For implementation of this policy a committee is made to frame the SOP to prevent such breaches in future. It has also been decided to hire Ministry of Electronics & Information Technology (MeitY) empaneled cloud services with provision of Disaster Recovery for hosting all web based applications after their security audit.

\*\*\*\*\*