GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 1635
TO BE ANSWERED ON: 29.07.2026

DATA BREACHES ON GOVERNMENT DIGITAL PLATFORMS

1635. SHRI S VENKATESAN:

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

(a) the number of instances of data breaches on Government digital platforms reported or detected during the last year;
(b) the details of specific corrective actions taken by the Government to address vulnerabilities highlighted in recent cyber-security audits; and
(c) the details of legal protocols and Standard Operating Procedures (SOPs) followed by the Government while sharing citizen data with law enforcement agencies?

ANSWER

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

(a) to (c): Government is committed to ensuring an open, safe, trusted and accountable cyberspace. Several legal, technical, and administrative policy measures have been implemented to address cyber security challenges in the country.

The Government has institutionalized a nationwide integrated and coordinated system to deal with cyber-attacks in the country which, inter alia, includes:

i. **The Indian Computer Emergency Response Team (CERT-In)** is designated as the national agency for responding to cyber security incidents under the provisions of section 70B of the Information Technology (IT) Act, 2000.
ii. CERT-In has created a panel of 'Information Security Auditing Organisations' for auditing, including vulnerability assessment and penetration testing of computer systems, networks, websites and applications of various organizations of the Government and critical sectors. 237 information security auditing organisations are empanelled by CERT-In to support and audit implementation of Information Security Best Practices.
iii. The vulnerabilities identified by the empanelled organisations during the initial audits are addressed by the respective entities through appropriate remediation measures, including patching and mitigation. Subsequently, the auditing organisations conduct revalidation audits to verify the effective closure of the identified vulnerabilities and assess compliance with the prescribed cybersecurity requirements and recommendations.
iv. CERT-In has developed and issued the "Comprehensive Cyber Security Audit Policy Guidelines" with the strategy to carry out cyber security audits in a consistent, effective, and secure manner across sectors including critical infrastructure.

v. CERT-In coordinates incident response measures with affected organisations, service providers, regulators and law enforcement agencies.

vi. **National Cyber Coordination Centre (NCCC)**, implemented by CERT-In, examines cyberspace to detect cyber security threats. It shares the information with concerned organizations, state governments and stakeholder agencies for taking action.

vii. CERT-In operates an automated cyber threat intelligence exchange platform for sharing tailored alerts with organisations across sectors for proactive threat mitigation.

viii. **Cyber Swachhta Kendra (CSK)**

- A citizen-centric service provided by CERT-In, which extends the vision of Swachh Bharat to the Cyber Space.
- It is the Botnet Cleaning and Malware Analysis Centre and helps to detect malicious programs and provides free tools to remove the same.
- It also provides cyber security tips and best practices for citizens and organisations.

ix. **Sectoral Computer Security Incident Response Team (CSIRT)**

- CSIRT in Finance sector (CSIRT-Fin) under CERT-In is operational since May 2020 to coordinate cyber incident response in the banking and financial sector.
- CSIRT-Power is operational since September 2024 as an extended arm of CERT-In to coordinate cyber security issues within the power sector entities.

x. CERT-In has formulated a Cyber Crisis Management Plan (CCMP) for countering cyber-attacks and cyber terrorism for implementation by all Ministries/Departments, State Governments and their organizations.

xi. Cyber security mock drills are conducted regularly by CERT-In, to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors.

xii. CERT-In has operationalised a Responsible Vulnerability Disclosure and Coordination Program for collection, analysis, mitigation and coordination with researchers/finders/vendors for fixing vulnerabilities in software/ devices.

xiii. CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, networks and data on an ongoing basis.

xiv. CERT-In conducts regular cyber security trainings, workshops for IT/ cyber security professionals of Government, public and private sector organizations.

xv. **Provisions under Digital Personal Data Protection Act, 2023**

- The Government has put in place a statutory framework under the Digital Personal Data Protection Act, 2023 and the rules framed thereunder to ensure that the sharing and processing of citizens' digital personal data for law enforcement purposes is undertaken in a lawful, secure and accountable manner.
- The Act recognises the sharing of personal data with another Data Fiduciary authorised by law to obtain such personal data, where the sharing is pursuant to a request made in writing for the prevention, detection or investigation of offences or cyber incidents, or for the prosecution or punishment of offences. It further provides for processing where personal data is processed in the

interest of prevention, detection, investigation or prosecution of any offence or contravention of any law for the time being in force in India.

- The Digital Personal Data Protection Rules, 2025 provide for reasonable security safeguards, including securing personal data through encryption, obfuscation, masking or the use of virtual tokens, reasonable measures for the detection of unauthorised access, retention of logs and other relevant data for the prescribed period, appropriate contractual provisions where a Data Processor is engaged, and appropriate technical and organisational measures to ensure effective observance of security safeguards.
- Accordingly, the framework under the Act and the Rules ensures that the sharing of citizens' personal data with law enforcement agencies is undertaken pursuant to lawful authority, through documented processes and subject to appropriate security safeguards and institutional accountability.

****