GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 2761
TO BE ANSWERED ON: 05.08.2026

INCIDENTS OF CYBER-ATTACKS

†2761. SHRI NARAYAN TATU RANE:
SHRI SANJAY UTTAMRAO DESHMUKH:
SMT. MANJU SHARMA:
SHRI SANJAY HARIBHAU JADHAV:

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

(a) the number of incidents of cyber-attacks on Government websites, digital platforms and critical infrastructure of the country from the year 2022 till date;
(b) the types and details of the said cyber-attacks;
(c) the number of cases of the said cyber-attacks in which sensitive data was compromised along with the details of action taken against the offenders particularly in Maharashtra;
(d) whether the Government considers the existing legal framework adequate to address the increasing number of cyber-attacks particularly in light of recent security breaches and if so, the details thereof;
(e) whether the Government plans to establish necessary infrastructure to provide enhanced security against growing cyber-attacks and if so, the details of the measures taken by the Government to formulate such plans to prevent such incidents in the future;
(f) the major steps taken by the Government to ensure the security of personal digital data; and
(g) the current status of the implementation of rules related to data protection?

ANSWER

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

(a) to (g): 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 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. As per the information reported to and tracked by CERT-In, the total number of cyber security incidents that belong to Central Ministries/Departments and State Governments, including those of Maharashtra, since 2022 is given below:

Year	Number
2022	192439
2023	204844
2024	1309372

2025	1821767
2026 (upto June)	1075220

On observing cyber security incidents, including those related to government-managed platforms, CERT-In coordinates incident response measures with affected organisations, service providers, regulators and law enforcement agencies.

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

i. **National Cyber Security Coordinator (NCSC)** under the National Security Council Secretariat (NSCS) to ensure coordination related to cyber security amongst different agencies.
ii. **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.
iii. **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.

iv. **Sectoral Computer Security Incident Response Team (CSIRT)**
- CSIRT in the finance sector (CSIRT-Fin) under CERT-In is operational from May 2020 to coordinate cyber incident response in the banking and financial sector.
- CSIRT-Power has been operational since September 2024 as an extended arm of CERT-In to coordinate cyber security issues within the power sector entities.

v. CERT-In operates an automated cyber threat intelligence exchange platform for sharing tailored alerts with organisations across sectors for proactive threat mitigation.
vi. 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.
vii. 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.
viii. 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.
ix. All the Government websites and applications are audited with respect to cyber security prior to their hosting. The auditing of the websites and applications is conducted on a regular basis after hosting also.
x. 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.
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 issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, networks and data on an ongoing basis.

xiii. **National Critical Information Infrastructure Protection Centre (NCIIPC**) has been established for protection of critical information infrastructure in the country under the provisions of section 70A of the Information Technology (IT) Act, 2000.

xiv. NCIIPC provides near real-time threat intelligence and situational awareness based on which regular alerts and advisories are sent to Critical Information Infrastructure (CII) / Protected System (PS) entities.

xv. NCIIPC undertakes vulnerabilities and risk assessment of Critical Information Infrastructure/ Protected Systems periodically and gives feedback to all concerned.

xvi. 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.
- The DPDP Rules are implemented in phases:

    i. Rules 1, 2 and 17 to 21 came into force upon publication in the Official Gazette in November 2025. These provisions cover the title and definitions of the Rules and matters relating to the appointment, service conditions, functioning and administration of the Data Protection Board.

    ii. Rule 4 relating to the registration and obligations of Consent Managers, is scheduled to come into force one year after publication, in November 2026.

    iii. Rules 3, 5 to 16, 22 and 23 are scheduled to come into force eighteen months after publication, in May 2027. These include the provisions relating to notices, reasonable security safeguards, personal data breach reporting, data retention, children's data, Significant Data Fiduciaries and the exercise of Data Principal rights.

****