GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 722
TO BE ANSWERED ON: 24.07.2026

STRENGTHENING OF CYBERSECURITY MECHANISMS

722. SHRI K.R.N. RAJESHKUMAR:

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

(a) whether cyber-attacks on Government institutions have increased;
(b) if so, the details thereof;
(c) whether Indian Computer Emergency Response Team (CERT-In) has strengthened cybersecurity mechanisms; and
(d) the details of action taken?

ANSWER

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

(a) to (d): The policies of Government of India are aimed at ensuring open, safe, trusted and accountable cyberspace for users in the country. The Government is cognizant and aware of various cyber security threats and challenges faced by Government institutions.

The Government has taken several measures to strengthen the cyber security mechanisms 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 coordinates incident response measures with affected organisations, service providers, regulators and law enforcement agencies.
iii. **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.
iv. CERT-In operates an automated cyber threat intelligence exchange platform for sharing tailored alerts with organisations across sectors for proactive threat mitigation.
v. **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.
vi. **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.

vii. CERT-In has empanelled 237 security auditing organisations to support and audit implementation of Information Security Best Practices.

viii. 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.

ix. 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.

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

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

xiii. **Advisories, Guidelines and Directions**

- CERT-In has issued a "Blueprint for Reducing Exposure and Defending against AI-Assisted Vulnerabilities Exploitation in Digital Infrastructure" in May 2026, aimed at protecting digital infrastructure against rapidly evolving AI-driven cyber threats.
- CERT-In has issued an advisory titled "Defending Against Frontier AI Driven Cyber Risks" in April 2026, outlined comprehensive measures for organizations, and individuals to strengthen protection against advanced AI-enabled threats.
- CERT-In has issued updated technical guidelines in July 2025 for Bill of Materials (BOM) for software, hardware, Artificial Intelligence, Quantum Computing & Cryptography requirements.
- 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.
- CERT-In has issued Cyber Security Directions in April 2022 under sub-section (6) of section 70B of Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet.

****