GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO.1498
TO BE ANSWERED ON: 31.07.2026

PROTECTION OF GOVERNMENT DIGITAL INFRASTRUCTURE AGAINST AI-ENABLED CYBER THREATS

1498. SHRI AKHILESH PRASAD SINGH:

Will the Minister of Electronics and Information Technology be pleased to state:

(a) whether Government has undertaken a comprehensive security audit of critical Government digital infrastructure against Artificial Intelligence-enabled cyber threats and ransomware attacks;
(b) whether vulnerabilities have been identified in digital public platforms and cloud-based Government services;
(c) the measures taken to strengthen cyber resilience, threat intelligence and incident response capabilities; and
(d) whether a national framework is under preparation to secure Government digital infrastructure against emerging cyber risks?

ANSWER

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

(a) to (d): Government is committed to ensuring an open, safe, trusted and accountable cyberspace. Several legal, technical and administrative policy measures have been taken to strengthen cyber resilience, threat intelligence and incident response capabilities, which inter alia include:

1. 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 Act, 2000.

2. 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.

3. 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.

4. 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.

5. Artificial Intelligence (AI) driven situational awareness systems are deployed by the CERT-In to detect malicious domains and phishing activities for necessary mitigation.

6. CERT-In has extended AI-enabled vulnerability assessment for public-facing digital assets in a sandbox environment to detect and mitigate vulnerabilities.
7. CERT-In coordinates incident response measures with affected organisations, service providers, regulators and law enforcement agencies.

8. **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.

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

10. **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.

11. **Sectoral Computer Security Incident Response Team (CSIRT)**
- CSIRT in the 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 has been operational since September 2024 as an extended arm of CERT-In to coordinate cyber security issues within the power sector entities.

12.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.

13. 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.

14.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.

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

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

******