GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 709
TO BE ANSWERED ON: 05.12.2025

CYBER SECURITY AND RESILIENCE

709. SHRI NARAYANASA K. BHANDAGE:
SMT. MAYA NAROLIYA:
SMT. KIRAN CHOUDHRY:
SHRI PRADIP KUMAR VARMA:
DR. MEDHA VISHRAM KULKARNI:
SHRI SUJEET KUMAR:

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

(a) the details of strategy for mandatory security audits for critical infrastructure units under CERT-In;
(b) the steps being taken by Ministry to address the increasing number of ransomware attacks and cross-border cyber-crime incidents;
(c) whether a National Cyber Resilience Fund (NCRF) has been established to strengthen the industry;
(d) the measures being taken to increase the number of certified cybersecurity professionals in the country; and
(e) the manner in which cybersecurity centres are being expanded to enhance regional cyber incident response effectiveness?

ANSWER

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

(a) to (e): Government of India is cognizant of the cyber threats to India's digital infrastructure. The policies of Government of India are aimed at ensuring a safe, trusted, and accountable cyberspace for all users.

Indian Computer Emergency Response Team (CERT-In) has developed and issued a Comprehensive Cyber Security Audit Policy Guidelines in July 2025 with the strategy to carry out cyber security audits in a consistent, effective, and secure manner across sectors including critical infrastructure. As per the guidelines, cyber security audit should be conducted at least once in a year.

CERT-In and National Critical Information Infrastructure Protection Centre (NCIIPC) carry out cybersecurity audits under Information Technology Act, 2000 and Rules made thereunder.

The Government has undertaken several measures to strengthen security of cyber ecosystem which, inter alia, includes:

(i) 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.

(ii) CERT-In issues alerts & advisories regarding latest cyber threats/vulnerabilities including malicious attacks using AI and countermeasures regularly. It advises remedial measures to affected organisations and coordinates incident response measures.

(iii) CERT-In has empanelled 231 security auditing organizations to support and audit implementation of Information Security Best Practices.

(iv) National Informatics Centre (NIC) carries out comprehensive security audit annually for its Critical Infrastructure to address the increasing number of ransomware attacks through CERT-In empanelled agencies including:

a) Information and Communication Technology infrastructure Audit of Central Ministries/Departments, States /UTs and National Data Centres.
b) Comprehensive Security Audit of Critical Web applications /databases /platforms.
c) Deployment of Unified Endpoint Management, Endpoint Detection and Response solutions across central ministries and departments for endpoint protection.
d) Removal of obsolete and legacy systems from the network.24×7 monitoring, detection, and mitigation of cyber threats using AI/ML and advanced security tools.
e) Continuous vulnerability assessments, system hardening, and proactive identification of application/system weaknesses.
f) Implementation of Zero Trust Security across NIC's ICT infrastructure.
g) Regular cybersecurity awareness programs for government employees.

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

(vi) The Certified Security Professional in Artificial Intelligence (CSPAI) program was launched by CERT-In in September 2024. The program aims to address the growing need for Secure and Responsible AI integration into business applications and processes. The CSPAI program equips cybersecurity professionals with the skills to secure AI systems, proactively address AI-related threats, and ensure trustworthy AI deployment in business environments.

(vii) Cyber security mock drills are conducted regularly to enable assessment of cyber security posture and preparedness of various organisations.

(viii) The Ministry of Electronics and Information Technology (MeitY) is implementing a project on 'Information Security Education and Awareness (ISEA)' for generating human resources in the area of Information Security and creating general awareness on various aspects of cyber hygiene/cyber security among the masses.

(ix) CERT-In has issued the necessary guidelines for setting up of State/sectoral Computer Security Incident Response Teams (CSIRTs). Sector-specific CSIRTs, such as CSIRT in Finance sector (CSIRT-Fin) and CSIRT in Power sector (CSIRT-Power) are operational to coordinate cyber security issues and improve cyber resilience within respective sectors.

******