GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 874
TO BE ANSWERED ON: 06.02.2026

MEASURES TO STRENGTHEN CYBER SECURITY

874. SHRI SUJEET KUMAR:

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

(a) the framework for mandatory security audits under Indian Computer Emergency Response Team (CERT-In), requiring critical infrastructure to transition from annual checks to continuous security assurance;
(b) the initiatives to counter ransomware and cross-border cybercrime, specifically the deployment of Artificial intelligence (AI)-based Unified Endpoint Management across Central Ministries;
(c) whether the ₹782 crore cybersecurity outlay (Budget 2025-26) serves as a National Cyber Resilience Fund to harden industry infrastructure;
(d) the steps under the Information Security Education and Awareness (ISEA) Phase-III to certify 10 lakh professionals by 2028; and
(e) the roadmap for scaling regional hubs for automated botnet cleaning?

ANSWER

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

(a) to (e): The policies of Government of India aim to ensure open, safe, trusted, and accountable Internet for all users.

Indian Computer Emergency Response Team (CERT-In) has developed and issued 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) regularly carry out cybersecurity audits.

The measures undertaken by government to ensure a resilient and secure cyber space, inter alia, include:

1. Empanelled 237 security auditing organizations by CERT-In to support and audit implementation of Information Security Best Practices.
2. National Informatics Centre (NIC) carries out following activities to address the increasing number of cyber threats including ransomware:
    i. Information and Communication Technology infrastructure (ICT) Audit of Central Ministries/Departments, States /UTs and National Data Centres.
    ii. Comprehensive Security Audit of Critical Web applications /databases /platforms.
    iii. Deployment of Unified Endpoint Management, Endpoint Detection and Response solutions across central ministries and departments for endpoint protection.

iv. 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.
v. Continuous vulnerability assessments, system hardening, and proactive identification of application/system weaknesses.
vi. Implementation of Zero Trust Security across NIC's ICT infrastructure.
vii. Regular cybersecurity awareness programs for government employees.

3. Ministry of Home Affairs (MHA) has established Indian Cybercrime Coordination Centre (I4C) to deal with cybercrimes in a coordinated and effective manner.
4. CERT-In coordinates incident response measures including for ransomware attacks with affected organisations, service providers, regulators and law enforcement agencies.
5. National Cyber Coordination Centre (NCCC) implemented by CERT-In, examines the cyberspace to detect cyber security threats. It shares the information with concerned organisations, state governments and stakeholder agencies for taking action.
6. AI driven situational awareness systems are deployed by CERT-In to detect malicious domains and phishing activities for necessary mitigation.
7. Cyber Crisis Management Plan formulated by CERT-In for countering cyber attacks and cyber terrorism for implementation by all Ministries/Departments.
8. CERT-In has issued a cyber security baseline document, in September 2025, which provides a minimum set of security controls recommended for Micro, Small and Medium Enterprises (MSMEs). This helps MSMEs to implement essential measures for strengthening their cyber security posture.
9. CERT-In conducts joint cyber security training programs in collaboration with Industry partners to upskill the cybersecurity workforce in Government, public and private organizations.
10. The budget of Rs. 782 Crore for FY 2025-26 is allocated by Ministry of Electronics and Information Technology (MeitY) to strengthen the security of the nation's cyberspace with focus on promotion of research & development, capacity building, enhancing indigenous skills and capabilities in the cyber security.
11. **Information Security Education & Awareness (ISEA):**
ISEA is an initiative for building human resources in Information Security and to spread cyber hygiene awareness among citizens. The key highlights are as under:

i. **Academic activities:** More than 4.05 lakh candidates trained in various formal/non-formal courses, innovation and other activities in Information Security since 2014 onwards.
ii. **Training of Government Officials:** 28,444 Government officials trained in various short-term programs in information security through direct/e-learning/Virtual Instructor Led Training (VILT) mode.
iii. **Mass Awareness:** 4,240 awareness workshops conducted across the country covering over 9.43 lakh participants, including school/college students, teachers, law enforcement, government personnel and general public. Around 15 crores estimated beneficiaries covered through indirect mode.

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

******