† **O.I.H.**

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 850
TO BE ANSWERED ON: 04.02.2026

CYBER SECURITY AUDIT OF DIGITAL GOVERNMENT SERVICES

†850. SHRI OMPRAKASH BHUPALSINH ALIAS PAVAN RAJENIMBALKAR:
SHRI SANJAY HARIBHAU JADHAV:

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

(a) whether the Government has conducted a cyber security audit of all digital Government services;
(b) if so, the details along with the findings thereof;
(c) the corrective measures taken by the Government based on the above findings;
(d) the measures currently being implemented to strengthen the security of digital Government platforms; and
(e) the additional steps proposed to protect digital Government services from cyber threats in the future?

ANSWER

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

(a) to (e): The policies of the Government of India aim to ensure a secure and trustworthy cyberspace while taking active measures to mitigate risk to India's digital infrastructure and Government services.

Indian Computer Emergency Response Team (CERT-In) and National Critical Information Infrastructure Protection Centre (NCIIPC) regularly carry out cybersecurity audits.

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

CERT-In has created a panel of 'Information Security Auditing Organisations' for auditing, including vulnerability assessments and penetration testing of computer systems, networks and applications of various organizations across sectors. Cyber security measures implemented by various organizations and its compliance with regulations are evaluated through periodic information security audits conducted by CERT-In empanelled organizations.

National Informatics Centre (NIC) carries out comprehensive annual cyber security audit of its critical applications, databases, and Information and Communication Technology (ICT) network infrastructure across Ministries, Departments, States, Union Territories and National Data Centres. Based on the audit

findings, the concerned entities undertake corrective measures to address the security gaps identified during the audit process.

The measures undertaken by government to strengthen security of digital Government platforms and services from cyber threats, inter alia, includes:

1. Comprehensive Cyber Security Audit Policy Guidelines have been issued by CERT-In in July 2025. As per these guidelines, cyber security audits are required to be conducted at least once every year in a consistent, effective, and secure manner across all sectors, including critical infrastructure.
2. Empanelled 237 security auditing organizations by CERT-In to support and audit implementation of Information Security Best Practices.
3. 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.
4. Alerts and advisories issued by CERT-In regarding latest cyber threats/vulnerabilities and countermeasures on an ongoing basis.
5. 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.

6. Cyber Crisis Management Plan formulated by CERT-In for countering cyberattacks and cyber terrorism for implementation by all Ministries/Departments.
7. A Responsible Vulnerability Disclosure and Coordination Program has been operationalised by CERT-In for the collection, analysis, and mitigation of vulnerabilities, including coordination with researchers, finders, and vendors for fixing vulnerabilities in software and devices.
8. CERT-In has issued guidelines for Secure Application Design, Development, Implementation & Operations to promote security-by-design across the application lifecycle.
9. 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.
10. Cyber security mock drills by CERT-In for assessment of cyber security posture and preparedness of organisations in Government and critical sectors.
11. Cyber security training programs conducted by CERT-In in collaboration with Industry partners to upskill the cyber security workforce in Government, public and private organizations. 23 and 32 training programs were conducted covering 12014 and 20799 participants during 2024 and 2025 respectively.
12. **National Cyber Security Awareness Activities**
    The Government organises events and activities for citizens as well as the technical cyber community across the country. Some of these include:

    - National Cyber Security Awareness Month (NCSAM) in October every year
    - Safer Internet Day on the second Tuesday of February

- Swachhta Pakhwada (1st –15th February), and
- Cyber Jagrookta Diwas (CJD) on the first Wednesday of every month
- Awareness resources are available on platforms like www.staysafeonline.in, www.infosecawareness.in, and www.csk.gov.in.

******