GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 3904
TO BE ANSWERED ON: 04.04.2025

CYBERSECURITY RESEARCH AND DIGITALINFRASTRUCTURE DEVELOPMENTIN ODISHA

3904. SHRIDEBASHISHSAMANTARAY:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:
(a) thestepstakentostrengthencybersecurityresearchanddigitalinfrastructurein Odisha;
(b) whether Government has set up any cybersecurity research centers or digital forensic labs in Odisha;
(c) the number of cybersecurity awareness programs conducted for industries andeducational institutions in Odisha; and
(d) the initiatives taken to promote data security and prevent cyber threats in Odisha's ITsector?

ANSWER

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

(a) to (d): The policies of the Government are aimed at ensuring an Open, Safe and Trusted and Accountable Internet for its users. The Government has taken following steps to strengthen cybersecurity research and digital infrastructure in the country including state of Odisha which, inter alia, includes:

(i) National Cyber Security Coordinator (NCSC) under the National Security Council Secretariat (NSCS) to ensure coordination amongst different agencies.
(ii) Under the provisions of section 70B of the Information Technology Act, 2000, the Indian Computer Emergency Response Team (CERT-In) is designated as the national agency for responding to cyber security incidents.
(iii) National Cyber Coordination Centre (NCCC) implemented by the CERT-In serves as the control room to scan the cyberspace in the country and detect cyber security threats. NCCC facilitates coordination among different agencies by sharing with them the metadata from cyberspace for taking actions to mitigate cyber security threats.
(iv) Cyber Swachhta Kendra (CSK) is a citizen-centric service provided by CERT-In, which extends the vision of Swachh Bharat to the Cyber Space. Cyber Swachhta Kendra is the Botnet Cleaning and Malware Analysis Centre and helps to detect malicious programs and provides free tools to remove the same, and also provides cyber security tips and best practices for citizens and organisations.
(v) Ministry of Home Affairs (MHA) has created Indian Cybercrime Coordination Centre (I4C) to deal with cybercrimes in a coordinated and effective manner.

(vi) Under the provisions of section 70A of the Information Technology (IT) Act, 2000, the Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country.

(vii) The Indian Computer Emergency Response Team (CERT-In) assists Odisha Government Ministries/ Departments/ Organizations in developing and implementing Cyber Crisis Management Plan (CCMP) document in line with national CCMP. The CCMP document is a strategic framework and set of guidelines designed to help entities prepare for, respond to, and initiate recovery from cyber incidents & crisis situations.

(viii) Regional Centre for Application Security and Audit is hosted at NIC (National Informatics Centre) Data Centre, Odisha to take proactive steps in securing the web applications.

(ix) Ministry of Electronics and Information Technology (MeitY) has acknowledged Research & Development (R&D) and promotion of innovation as an integral part of the Cyber Security ecosystem, supporting the entire value chain of R&D activities in the country, ranging from basic components to sophisticated product development. MeitY has taken various initiatives to promote R&D in different areas including Cyber Security and digital forensics.

The Government conducts cyber security awareness programs for industries and educational institutions, including those for state of Odisha, which, inter-alia, includes:

(i) CERT-In conducts regular training programmes for IT and cyber security professionals of government and critical sector organisations regarding securing information technology infrastructure and mitigating cyber attacks. A total of 12,014 officials have been trained in 23 training programs in 2024, including 177 officials from Odisha.

(ii) On International Women's Day 2025, 21 women officials from Odisha took part in CERT-In's "Cybersecurity Awareness Sessions for Women Officials." Through a combination of engaging quizzes, dynamic interactive lectures, and insightful discussions, participants learned from prominent women experts from CERT-In and Industry.

(iii) In the year 2025 a total of 41 cybersecurity awareness programs have been conducted on Safer Internet Day (11th Feb 2025) covering all Districts and State HQ by NIC Odisha. NIC also conducts Panel discussions on Cyber Security over All India Radio and TV Channels.

(iv) National Institute of Electronics and Information Technology (NIELIT) is an autonomous scientific society under the administrative control of the Ministry of Electronics and Information Technology (MeitY), Government of India. NIELIT Bhubaneswar conducts various workshops and seminars, especially during National Cyber Security Awareness Month (NCSAM), to raise awareness about cyber threats, security issues, and best practices. It has implemented initiatives like the CyberShiksha program to educate the public, including students and government employees.

(v) NIELIT Bhubaneswar offers courses focused on data security and cyber threat prevention including 300 hrs National Skills Qualifications Framework (NSQF) aligned course on cyber security assistant and other relevant programs. It is also running course namely "Foundation course in Cyber Security" at various district level like Ganjam, Balasore, Khorda, Nuapada, Jagatsinghpur, etc.

(vi) 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. Under the project, 4,192 candidates have been trained/under-going in formal/non-formal courses in Information Security by two institutions namely, National Institute of Technology Rourkela and International Institute of Information Technology, Bhubaneswar. Under the awareness activity, 3,583 awareness workshops on Information Security have been organized through direct/virtual mode across the country for various users covering 8,12,740 participants, out of which 133 awareness workshops have been organized in Odisha covering 26,369 participants.

(vii) MeitY conducts programmes to generate information security awareness. Awareness material in the form of handbooks, short videos, posters, brochures, cartoon stories for children, advisories, etc. on various aspects of cyber hygiene & cyber security including deepfakes are disseminated through portals such as www.staysafeonline.in, www.infosecawareness.in and www.csk.gov.in.

The Government is cognizant of various cyber security threats and challenges in the country. Government has taken several legal, technical, and administrative policy measures for addressing cyber security challenges in the country. Government has taken following steps to promote data security and prevent cyber threats in the country which, inter-alia, includes:

(i) To ensure data security, web applications are audited prior to their deployment by NIC Data Centre at Odisha. It also undertakes post deployment compliance checks of hosted applications and their infrastructure on periodic basis.

(ii) CERT-In 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.

(iii) CERT-In issued Guidelines for Secure Application Design, Development, and Implementation & Operations in September 2023. CERT-In has also released the Software Bill of Materials (SBOM) guidelines for entities, particularly those in the public sector, government, essential services, organizations involved in software export and software services industry in October 2024 to help organizations know exactly what components are in their software or assets, making it easier to identify and fix vulnerabilities.

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

(v) National Cyber Coordination Centre (NCCC) implemented by the CERT-In serves as the control room to scan the cyberspace in the country and detect cyber security

threats. NCCC facilitates coordination among different agencies by sharing with them the metadata from cyberspace for taking actions to mitigate cyber security threats.

(vi) CERT-In operates an automated cyber threat intelligence exchange platform for proactively collecting, analysing and sharing tailored alerts with organisations across sectors for proactive threat mitigation actions by them.

(vii) CERT-In has empanelled 200 security auditing organisations to support and audit implementation of Information Security Best Practices.

(viii) Cyber security mock drills are conducted regularly to enable assessment of cyber security posture and preparedness of organisations and enhance resilience in Government and critical sectors. 109 such drills have so far been conducted by CERT-In where 1438 organizations from different States and sectors participated.

(ix) NCIIPC (National Critical Information Infrastructure Protection Centre) provides threat intelligence, situational awareness, alerts & advisories and information on vulnerabilities to organisations having Critical Information Infrastructure (Clls)/ Protected Systems (PSs) for taking preventive measures from cyber-attacks and cyber terrorism.

(x) NIC provides Information Technology (IT) support to ministries, departments and agencies of the Central Government, State Governments and district administrators for various e-governance solutions and follows information security policies and practices in line with industry standards and practices, aimed at preventing cyber-attacks and safeguarding data.

(xi) NIC has deployed advanced security tools including Threat Intelligence Platform to identify the security issues associated with Government network.

******