GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS

LOK SABHA
UNSTARRED QUESTION NO. 5065

TO BE ANSWERED ON THE 24TH MARCH, 2026/ CHAITRA 3, 1948 (SAKA)

ASSISTANCE TO STATES TO TACKLE CYBER INCIDENTS

5065. SHRI DAGGUMALLA PRASADA RAO:

Will the Minister of HOME AFFAIRS be pleased to state:

(a) the details regarding the number of cyber incidents reported in the country during the last five years, year-wise;

(b) the States reporting the highest number of cyber-incidents, along with details of any special assistance, capacity-building or technical support provided by the Central Government to such vulnerable States;

(c) the details regarding the estimated financial loss accrued due to cyber-incidents during the said period, year-wise;

(d) the details of the number of persons or organizations convicted for cyber crimes during the last five years and the amount recovered from such cases, year-wise; and

(e) the measures taken by the Government to strengthen cyber-crime investigation, digital forensics and inter-agency coordination across States?

ANSWER

MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS
(SHRI BANDI SANJAY KUMAR)

(a) to (c): 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. As per the information reported to and tracked by CERT-In, the total number of cyber security incidents observed during the last five years are given below:

Year	Number of cyber security incidents
2021	14,02,809
2022	13,91,457
2023	15,92,917
2024	20,41,360
2025	29,44,248

As per CERT-In, the highest number of cyber incidents reported including from sectors are from National Capital Territory of Delhi. Details regarding the estimated financial loss accrued due to cyber-incidents is not maintained by the CERT-In.

CERT-In has taken following measures to provide assistance to all States and UTs for enhancing cyber security and prevent cyber attacks:

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

ii. **National Cyber Coordination Centre (NCCC) implemented by CERT-In, examines the cyberspace to detect cyber security threats. It shares the information with concerned State Governments, organisations across sectors, and stakeholder agencies for taking action.**

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

iv. Cyber Swachhta Kendra (CSK) is a service provided by CERT-In, which extends the vision of Swachh Bharat to the cyber space. Cyber Swachhta Kendra helps to detect malicious programs and vulnerable services and provide remedial measures to organisations across States and sectors.

v. CERT-In has empanelled 237 security auditing organisations to support and audit implementation of Information Security Best Practices.

vi. Cyber security mock drills are conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government (Central & States) and critical sectors. Workshops along with these drills are conducted in States for facilitating coordination and information sharing in the area of cyber security.

vii. CERT-In has launched a specific cybersecurity program “Cyber Bharat Setu” which focuses on promoting cybersecurity culture in States/UTs. Madhya Pradesh, Tripura, Uttarakhand and Jammu & Kashmir Administration participated in this program in 2025.

viii. CERT-In conducts joint cyber security training programs in collaboration with Industry partners to upskill the cyber security workforce in Government (Central & States), public and private organizations across sectors.

(d) & (e): 'Police' and 'Public Order' are State subjects as per the Seventh Schedule of the Constitution of India. The States/UTs are primarily responsible for the prevention, detection, investigation, complaint reporting, recovery actions, victim support systems and prosecution of crimes including cyber fraud through their Law Enforcement Agencies (LEAs). The Central Government supplements the initiatives of the States/UTs through advisories and financial assistance under various schemes for capacity building of their LEAs.

The National Crime Records Bureau (NCRB) compiles and publishes the statistical data on crimes in its publication "Crime in India". The latest published report is for the year 2023. As per the data published by the NCRB, year wise details of cases registered and persons convicted under cyber crimes (involving communication devices as medium/target) during the period from 2019 to 2023 are at below:

Year	Cases Registered	Persons Convicted
2019	44735	486
2020	50035	1369
2021	52974	736
2022	65893	1407
2023	86420	1104

The data on amount recovered is not maintained by the NCRB.

To strengthen the mechanism to deal with cyber crimes in a comprehensive and coordinated manner, the Central Government has taken steps which, inter-alia, include the following:

i. **The Ministry of Home Affairs has set up the 'Indian Cyber Crime Coordination Centre' (I4C) as an attached office to deal with all types of cyber crimes in the country, in a coordinated and comprehensive manner.**

ii. **The 'National Cyber Crime Reporting Portal' (NCRP) (https://cybercrime.gov.in) has been launched, as a part of the I4C, to enable public to report incidents pertaining to all types of cyber crimes, with special focus on cyber crimes against women and children. Cyber crime incidents reported on National Cyber Crime Reporting Portal, their conversion into FIRs and subsequent action i.e. filing of chargesheets, arrest and resolution of complaints, thereon are handled by the State/UT Law Enforcement Agencies concerned as per the provisions of the law.**

iii. The 'Citizen Financial Cyber Fraud Reporting and Management System' (CFCFRMS), under I4C, has been launched in year 2021 for immediate reporting of financial frauds and to stop siphoning off funds by the fraudsters. As per CFCFRMS operated by I4C, till 31.01.2026, financial amount of more than Rs. 8,690 Crore has been saved in more than 24.65 lakh complaints. A toll-free Helpline number '1930' has been operationalized to get assistance in lodging online cyber complaints.

iv. A State of the Art, Cyber Fraud Mitigation Centre (CFMC) has been established at I4C where representatives of major banks, Financial Intermediaries, Payment Aggregators, Telecom Service Providers, IT Intermediaries and representatives of States/UTs Law Enforcement Agency are working together for immediate action and seamless cooperation to tackle cybercrime.

v. I4C, MHA is regularly organising 'State Connect', 'Thana Connect' and Peer learning session to share best practices, enhance capacity building, etc.

vi. The state of the art National-Digital Investigation Support Centre (previously known as National Cyber Forensic Laboratory (Investigation) {NCFL(I)}) has been established, as a part of the I4C, at New Delhi (on 18.02.2019) and at Assam (on 29.08.2025) to provide early stage cyber

forensic assistance to Investigating Officers (IOs) of State/UT Police. Till 31.01.2026, National-Digital Investigation Support Centre, New Delhi has provided its services to State/UT LEAs in more than 13,417 cases pertaining to cyber crimes.

vii. The Ministry of Home Affairs has released financial assistance to the tune of Rs. 132.93 crores under the 'Cyber Crime Prevention against Women and Children (CCPWC)' Scheme, to the States/UTs for their capacity building such as setting up of cyber forensic-cum-training laboratories, hiring of junior cyber consultants and training of LEAs' personnel, public prosecutors and judicial officers. Cyber forensic-cum-training laboratories have been commissioned in 33 States/UTs and more than 24,600 LEA personnel, judicial officers and prosecutors have been provided training on cyber crime awareness, investigation, forensics etc.

viii. The Massive Open Online Courses (MOOC) platform, namely 'CyTrain' portal has been developed under I4C, for capacity building of police officers/judicial officers through online course on critical aspects of cyber crime investigation, forensics, prosecution etc. Till 31.01.2026, more than 1,51,081 police officers/judicial officers from States/UTs are registered and more than 1,42,025 Certificates issued through the portal.

ix. A Suspect Registry of identifiers of cyber criminals has been launched by I4C on 10.09.2024 in collaboration with Banks/Financial Institutions. Till 31.01.2026, more than 23.05 lakh suspect identifier data received from Banks and 27.37 lakh Layer 1 mule accounts have been shared with the participating entities of Suspect Registry and declined transactions worth Rs. 9518.91 crores.

x. Seven Joint Cyber Coordination Teams (JCCTs) have been constituted for Mewat, Jamtara, Ahmedabad, Hyderabad, Chandigarh, Vishakhapatnam, and Guwahati under I4C covering the whole country based upon cyber crime hotspots/ areas having multi jurisdictional issues by onboarding States/UTs to enhance the coordination framework among the Law Enforcement Agencies of the States/UTs.

xi. Samanvaya Platform has been made operational to serve as an Management Information System (MIS) platform, data repository and a coordination platform for LEAs for cybercrime data sharing and analytics. It provides analytics based interstate linkages of crimes and criminals, involved in cybercrime complaints in various States/UTs. The module 'Pratibimb' maps locations of criminals and crime infrastructure on a map to give visibility to jurisdictional officers. The module also facilitates seeking and receiving of techno-legal assistance by Law

Enforcement Agencies from I4C and other SMEs. It has lead to arrest of more than 21,857 accused and more than 1,49,636 Cyber Investigation assistance request.

xii. A comprehensive Standard Operating Procedure (SOP) has been issued by the Central Government on 2nd January 2026. It provides a uniform, victim-centric framework for handling complaints through the National Cybercrime Reporting Portal (NCRP) and Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS). The Standard Operating Procedure (SOP) for NCRP-CFCFRMS outlines a dedicated Coordination Mechanism to enhance collaboration, particularly with States and Union Territories, whose police agencies are integral stakeholders in the system.

*****