

**GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS**

**RAJYA SABHA
UNSTARRED QUESTION NO. 403**

TO BE ANSWERED ON THE 22ND JULY, 2026/ ASHADHA 31, 1948 (SAKA)

NATIONAL CYBERCRIME RESPONSE MECHANISM

403 SHRI G.C. CHANDRASHEKHAR:

Will the Minister of HOME AFFAIRS be pleased to state:

- (a) the State-wise number of cybercrime complaints, FIRs registered, amount involved, amount frozen and amount recovered through the Indian Cyber Crime Coordination Centre (I4C) during financial year 2023-24 to financial year 2025-26;**
- (b) whether Government has assessed the average time taken by law enforcement agencies to freeze fraudulently transferred funds; and**
- (c) the measures taken to strengthen Inter-State coordination and digital forensic capacity?**

ANSWER

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

(a) to (c) : 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.

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.

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 30.06.2026, financial amount of more than Rs. 11,158 Crore has been saved in more than 32.80 lakh complaints. A toll-free Helpline number '1930' has been operationalized to get assistance in lodging online cyber complaints. As per NCRP & CFCFRMS operated by I4C, from the financial years 2023–24 to 2025–26, the total number of cyber fraud complaints on NCRP are more than 5387905, the total number of FIRs registered is more than 181271, the total amount reported is more than ₹ 56087 crores, the total amount marked as Lien is more than ₹ 9079 crores, and the amount refunded is more than ₹ 206 crores.

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.

To further strengthen operational efficiency and ensure uniformity in handling cybercrime complaints, the Ministry has issued a comprehensive Standard Operating Procedure (SOP) for NCRP-CFCFRMS. The SOP lays down a standardized framework for complaint processing, bank coordination,

grievance redressal, removal of lien markings, and restoration of defrauded funds to rightful claimants based on complaints received through the NCRP. Money Restoration Module for expeditious restoration of defrauded money to the victims and Grievance Redressal Module for timely attending to the grievances relating to freezing of the bank accounts and lien marking of the amount, have been made functional from April, 2026.

The Central Government continuously monitors the average time taken by law enforcement agencies and financial institutions to freeze fraudulently transferred funds. Real time action is ensured through API integration between the CFCFRMS and Financial Institutions for immediately blocking the defrauded amounts.

The Central Government has taken the following steps to strengthen inter state coordination and digital forensic capacity:

- i. 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.**

- ii. 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 29,837 accused and more than 2,33,593 Cyber Investigation assistance request.**
- iii. 'Sahyog' Portal has been launched to expedite the process of sending notices to IT intermediaries by the Appropriate Government or its agency under clause (b) of sub-section (3) of section 79 of the IT Act, 2000 to facilitate the removal or disabling of access to any information, data or communication link being used to commit an unlawful act.**
- iv. A Suspect Registry of identifiers of cyber criminals has been launched by I4C on 10.09.2024 in collaboration with Banks/Financial Institutions. Till 30.06.2026, more than 30.48 lakh suspect identifier data received from Banks and 32.08 lakh Layer 1 mule accounts have been shared with the participating entities of Suspect Registry and declined transactions worth Rs. 25,698 crores.**

- v. 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.**
- vi. I4C, MHA is regularly organising ‘State Connect’, ‘Thana Connect’ and Peer learning session to share best practices, enhance capacity building, etc.**
- vii. 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 30.06.2026, National-Digital Investigation Support Centre, New Delhi has provided its services to State/UT LEAs in more than 14,064 cases pertaining to cyber crimes.**
- viii. 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.

- ix. At present, 07 Central Forensic Science Laboratories and 28 State Forensic Science Laboratories are operational across the country to assist in investigation of cybercrime cases. Assistance has been provided to 20 States / UTs inter-alia for Strengthening of Cyber Forensic Capacities in State FSLs under the Nirbhaya funded scheme for Strengthening of DNA Analysis and Cyber Forensic Capacities in State FSLs.**
