

**GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS**

**RAJYA SABHA
UNSTARRED QUESTION NO. 1188**

TO BE ANSWERED ON THE 29TH JULY, 2026/ SHRAVANA 7, 1948 (SAKA)

CYBER CRIME COORDINATION CENTRE

1188 # DR. DINESH SHARMA:

Will the Minister of HOME AFFAIRS be pleased to state:

(a) whether the Indian Cyber Crime Coordination Centre has been established for the coordination of efforts to combat cyber crime;

(b) whether it is effective in combating cyber crime; and

(c) the other measures taken by Government to deal with all forms of cyber crime in a comprehensive and coordinated manner?

ANSWER

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

(a) to (c) : Ministry of Home Affairs (MHA) established Indian Cyber Crime Coordination Centre (I4C) as scheme in the year 2018 to evolve a framework and ecosystem for the prevention, detection, investigation and prosecution of cybercrime in the country. In a short span I4C has worked towards enhancing the nation's collective capability to tackle cybercrimes and develop effective coordination among the Law Enforcement Agencies. I4C has been set up as an Attached Office of MHA with effect from 1st July, 2024. I4C focuses on tackling all the issues related to Cybercrime for the citizens, which includes improving coordination between various Law

Enforcement Agencies and the stakeholders, capacity building, awareness etc.

‘Police’ and ‘Public Order’ are State subjects under the Seventh Schedule to the Constitution of India. Accordingly, the States and Union Territories (UTs) are primarily responsible for the prevention, detection, investigation, and prosecution of cybercrime. The Central Government, through the Ministry of Home Affairs (MHA), supplements the efforts of States and UTs by providing policy guidance, technological support, capacity-building assistance, and financial resources to strengthen cybercrime management and enforcement capabilities.

The Central Government has taken the following measures to deal with all forms of cyber crime in a comprehensive and coordinated manner:

- i. National Cyber Crime Reporting Portal (NCRP): A citizen-centric platform for online reporting of cybercrime complaints, enabling prompt registration and action by the concerned law enforcement agencies.**
- ii. National Helpline 1930: A dedicated helpline for reporting cyber financial frauds and facilitating immediate response.**
- iii. Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS): A mechanism for immediate reporting of financial cyber**

frauds and timely intervention to prevent the diversion or siphoning of defrauded funds.

- iv. Samanvaya Platform: Developed for facilitating inter-State coordination and cybercrime analytics.**
- v. 'Sahyog' Portal to facilitate the removal or disabling of unlawful content.**
- vi. Seven Joint Cyber Coordination Teams (JCCTs) have been constituted to act upon cyber crime hotspots.**
- vii. Suspect Registry: A national repository containing over 30.48 lakh suspect identifiers, including mobile numbers, bank accounts, and other digital identifiers associated with cybercriminal activities.**
- viii. Cyber Fraud Mitigation Centre (CFMC): A collaborative platform comprising representatives from Banks, Financial Intermediaries, Law Enforcement Agencies, Telecom Service Providers, IT Intermediaries, and I4C for coordinated action against cyber-enabled financial frauds.**
- ix. Cyber Commando programme for the creation of a dedicated, skilled workforce capable of securing critical information infrastructure and supporting national cybersecurity efforts.**
- x. The National-Digital Investigation Support Centre has been established 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.**

- xi. Capacity Building and Public Awareness: Regular training programmes for law enforcement personnel and extensive public awareness campaigns through SMS alerts, social media platforms, and other outreach initiatives to enhance cyber hygiene and digital safety awareness.**
- xii. 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.**
