

**GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS**

**LOK SABHA
UNSTARRED QUESTION NO. 1443**

TO BE ANSWERED ON THE 28TH JULY, 2026/ SHRAVANA 6, 1948 (SAKA)

CFCFRMS 2.0 PLATFORM

**1443. ADV GOWAAL KAGADA PADAVI:
 SHRI VISHALDADA PRAKASHBAPU PATIL:
 DR. BACHHAV SHOBHA DINESH:**

Will the Minister of HOME AFFAIRS be pleased to state:

(a) whether the Ministry has operationalized the "CFCFRMS 2.0" platform to enable the realtime freezing of fraudulent transactions across all scheduled banks;

(b) whether the National Cyber Helpline (1930) has achieved a success rate of over 90% in intercepting stolen funds before they are moved out of the banking system;

(c) whether the Ministry has deployed an AI-based "Cyber-Threat Early Warning System" to alert citizens against sophisticated phishing and deep-fake scams;

(d) whether the government has established dedicated Cyber Forensic Labs in every district across the country to expedite the investigation of digital crimes particularly in Maharashtra; and

(e) whether the Ministry is collaborating with international financial gateways to recover funds siphoned to offshore accounts by transnational cyber syndicates?

ANSWER

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

(a) to (e) The ‘Citizen Financial Cyber Fraud Reporting and Management System’ (CFCFRMS), under Indian Cyber Crime Coordination Centre 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.

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.

‘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, and prosecution of crimes including establishment of cyber forensic laboratories 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.

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.

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.

CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities including malicious attacks using Artificial

Intelligence and countermeasures to protect computers, networks and data on an ongoing basis.

AI driven situational awareness systems are deployed by CERT-In to detect malicious domains and phishing activities for necessary mitigation.

CERT-In operates an automated cyber threat intelligence exchange platform for sharing tailored alerts with organisations across sectors for proactive threat mitigation.

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 including Maharashtra and more than 24,600 LEAs personnel, judicial officers and prosecutors have been provided training on cyber crime awareness, investigation, forensics etc.

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.

At present, 07 Central Forensic Science Laboratories and 28 State Forensic Science Laboratories including in Maharashtra are operational across the country to assist in investigation of cybercrime cases. Assistance has been provided to 20 States / UTs 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.

Till 30.06.2026, a total of 1,586 entities have been onboarded onto the CFCFRMS platform, including 40 foreign banks operating in India.
