

CYBER SECURITY INFRASTRUCTURE

प्रविष्टि तिथि: 02 DEC 2025 3:24PM by PIB Delhi

The Government has institutionalized a nationwide integrated and coordinated system to deal with cyber threats. National Cyber Security Coordinator (NCSC) under the National Security Council Secretariat (NSCS) ensures coordination amongst different agencies whereas Indian Cybercrime Coordination Centre (I4C) deals with cybercrimes in a coordinated and effective manner.

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 (IT) Act, 2000. CERT-In operates an automated cyber threat intelligence exchange platform for sharing tailored alerts with organization across sectors for proactive threat mitigation. National Cyber Coordination Centre (NCCC) implemented by CERT-In, examines the cyberspace to detect cyber security threats. It shares the information with concerned organizations, state governments and stakeholder agencies for taking action. CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities from time to time.

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

Ministry of Home Affairs (MHA) has established CyMAC (Cyber Multi Agency Centre) under the MAC (Multi Agency Centre) platform with participating agencies viz. IB, CIRA, DCYA, DoT, Cert-In, I4C, NCIIPC and NIC, to effectively address cybercrime, cyber espionage, cyber terrorism, cyber security threats, misuse of emerging technologies against national security and similar concerns. The CyMAC platform serves as a unified and strategic platform to enhance cyber resilience across all Cyber Security Agencies. By enabling real-time monitoring, threat intelligence sharing, and coordinated response capabilities, it ensures the proactive detection & analysis and collaborative approach to manage cyber security risks effectively. All agencies are being encouraged to fully integrate with this system to strengthen National Cyber Defence and safeguard Indian Information and Communication Technology (ICT) infrastructure.

A new National Cyber Forensic (Investigation) Laboratory has been set up in Assam, to provide cyber forensic facilities and enhance digital investigation capabilities of all LEAs mainly working in North East Region and Sikkim. This is operationalized since 29.08.2025.

National Cyber Forensic (Investigation) Laboratory {NCFL(I)}, a 'State-of-the-Art' facility has been set up at Dwarka, New Delhi under the Indian Cyber Crime Coordination Centre(I4C) in 2019 to provide forensic assistance during investigation to LEAs and other central agencies. NCFL services or facilities

are being utilized by States/UTs across the country. Till 31.10.2025, NCFL have provided its services to State LEAs in around 12,952 cyber cases pertaining to cybercrime. Till, 31.10.2025, 2118 LEAs personal have been trained on latest forensic tools and techniques.

Cyber Forensic Labs in States/UTs had been set up under Cyber Crime Prevention against Women and Children (CCPWC) Scheme which was launched in 2018. Under this Scheme, MHA had provided financial assistance to the tune of Rs. 131.60 crores to States/UTs for setting up of Cyber Forensic Consultants. Cyber Forensic-cum-Training Laboratories have been commissioned in 33 States/UTs.

CERT-In conducts workshops along with drills in states including North-Eastern region for facilitating coordination and information sharing in the area of cyber security.

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

Samanvaya Platform has been made operational to serve as an Management Information System (MIS) platform, data repository and a coordination platform for Law Enforcement Agencies (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 16,840 accused and 1,05,129 Cyber Investigation assistance request.

The Massive Open Online Courses (MOOC) platform, namely 'CyTrain' to build the capacity of police and judicial officers in cyber crime investigation, forensics, and prosecution. It offers standardized online courses with certification, ensuring uniform skill development across agencies. 1,44,895 Police officers/Judges/Prosecutors/CPO/CAPFs are registered and 1,19,628 Certificates issued through the portal till 31.10.2025.

This was stated by the Minister of State in the Ministry of Home Affairs Shri Bandi Sanjay Kumar in a written reply to a question in the Lok Sabha.

RK/RR/SJK/PS/PR/PS

(रिलीज आईडी: 2197529) आगंतुक पटल : 1685

इस विज्ञप्ति को इन भाषाओं में पढ़ें: Urdu , हिन्दी , Assamese , Tamil , Telugu