



PRAJWALA

Draft National Plan of Action To Combat Cyber-Enabled Human Trafficking (NPoA-CENT)

(Prepared in consultation with Law Enforcers, Judicial Officers,
Prosecutors, Women & Child Welfare Officers and Civil Society Organisations)

Designed by
Sreenuarts

Printed at
Pragathi Art Printers
www.pragathi.com

Cover Design
Rajesh Touchriver



Draft National Plan of Action To Combat Cyber-Enabled Human Trafficking (NPoA-CEHT)

**(Prepared in consultation with Law Enforcers, Judicial Officers,
Prosecutors, Women & Child Welfare Officers and Civil Society
Organisations)**

Table of Contents

	Page No.
1. Introduction	1
2. Need for National Plan of Action	6
3. Process adopted for drafting National Plan of Action	7
4. Guiding Principles	8
5. Objectives of NPoA CEHT	9
6. Structure and Flow of NPoA	10
i) Institutional Framework	11
ii) Prevention	14
iii) Crime Detection	19
iv) Investigation	22
v) Prosecution	25
vi) Victim Protection	27
vii) Legal Reforms	30
viii) Capacity Building	31
ix) Monitoring Mechanism	34
7. Annexure - List of Contributors	35

Abbreviations

AHTUs	Anti-Human Trafficking Units
AI	Artificial Intelligence
ASHA	Accredited Social Health Activist
BCI	Bar Council of India
BNS	Bhartiya Nyaya Sanhita
BNSS	Bharatiya Nagarik Suraksha Sanhita
BPR&D	Bureau of Police Research and Development
CBI	Central Bureau of Investigation
CEHT	Cyber-Enabled Human Trafficking
CERT-In	Indian Computer Emergency Response Team
CLPR Act	Child Labour (Prohibition and Regulation) Act
CPCR Act	Commissions for Protection of Child Rights Act
CSAM	Child Sexual Abuse Material
CSOs	Civil Society Organisations
CSR	Corporate Social Responsibility
DAHTU	District Anti Human Trafficking Unit
DMC	District Monitoring Cell
DRDA	District Rural Development Agency
FIU-IND	Financial Intelligence Unit-India
I & B	Ministry of Information and Broadcasting
I4C	Indian Cyber Crime Coordination Centre
ICJS	Inter-Operable Criminal Justice System
IMCC	Inter-Ministerial Coordination Council
IT Act	Information Technology Act
ITPA	Immoral Traffic (Prevention) Act
IVSCs	Integrated Victim Support Centres
JJ Act	Juvenile Justice (Care and Protection of Children) Act
LEAs	Law Enforcement Agencies
MEA	Ministry of External Affairs
MeitY	Ministry of Electronics and Information Technology
MEL	Monitoring, Evaluation, and Learning
MFSU	National Forensic Sciences University

MHA	Ministry of Home Affairs
MoCA	Ministry of Civil Aviation
MoE	Ministry of Education
MoHFW	Ministry of Health and Family Welfare
MOIA	Ministry of Overseas Indian Affairs
MOL&E	Ministry of Labour and Employment
MoL& J	Ministry of Law & Justice
MoRD	Ministry of Rural Development
MSJE	Ministry of Social Justice and Empowerment
MSME	Ministry of Micro, Small and Medium Enterprises
MWCD	Ministry of Women & Child Development
NCC	National Coordination Centre
NCR&IC	National Cyber-Crime Research & Innovation Centre
NCRB	National Crime Records Bureau
NIA	National Investigation Agency
NIC	National Informatics Centre
NJA	National Judicial Academy
NPA	National Police Academy
NPoA	National Plan of Action
NSDC	National Skill Development Corporation
PLC	Panchayat-Level Committee
POCSO	Protection of Children from Sexual Offences Act
PRI	Panchayat Raj Institutions
PSA	Public Service Announcement
RBI	Reserve Bank of India
SCC	State Coordination Centre
SOPs	Standard Operating Procedures
TRAI	Telecom Regulatory Authority of India
UGC	University Grants Commission
UNTOC	United Nations Convention against Transnational Organized Crime

I. Introduction

Technological advancements have revolutionised virtually every aspect of human life. Central to this transformation has been the proliferation of digital technologies. The two phenomena, which are the widespread availability of high-speed internet connectivity and the proliferation of mobile apps, have taken information exchange to unprecedented levels, leading to the democratisation of technology and empowering individuals to participate in the digital economy like never before. This accelerated pace of technological adoption has enabled individuals to access information and services easily. Applications thriving on such technological advances, such as social media platforms, have given new meaning to forging associations, sharing and engaging with content, and fostering virtual communities and networks that transcend geographic boundaries. AI powered algorithms are increasingly being used to automate tasks, optimise processes, and personalise experiences, transforming how businesses operate, and individuals interact with technology.

Unfortunately, this technological advancement also has a dark side. Digital platforms have offered safe havens to criminal elements who exploit these platforms for illicit activities. Cyberspace is the new crime scene, enabling fraud, identity theft, doxing, morphing, phishing, and many other crimes, including Cyber-Enabled Human Trafficking (CEHT). The anonymity, accessibility, and dynamic nature of the internet have facilitated the perpetration of crimes on an unprecedented scale globally.

Over the past few decades, trafficking in persons as a crime has expanded and manifested into various forms. The entry of technology, and the dynamics of technology-supported human trafficking have taken this global scourge to new levels. Technology has become a tool for traffickers to facilitate, organise, network, transact and evade authorities with greater speed, less cost and more anonymity.

Between January and April 2024, India lost significant amounts to cyber scams: ₹14,25,827,200 (US\$16.96 million) from investment scams, ₹2,22,775,500 (US\$2.65 million) from trading scams, and millions more from digital arrest and dating scams, according to I4C¹. Reports indicate these scams, originating from Southeast Asia, are part of organised crime networks tied to cyber-enabled human trafficking wherein trafficked victims are forced to commit such crimes.

Prajwala, a leading anti-trafficking organisation conducted extensive, on-ground research in 2024 to explore the evolving landscape of CEHT. This involved wide-ranging consultations with leading global experts, gathering data from law enforcement officials, conducting validation investigations, interactions with survivors, interactions with civil society organisations, and extensive secondary research.

¹www.orfonline.org/expert-speak/cyber-scams-and-trafficking-india-s-southeast-asian-challenge#:~:text=According%20to%20the%20Indian%20Cyber,US%241.43%20million%20from%204%2C600

The major findings of the research captured in a document titled “The National Action Research Report” are summarised as follows:

A. Problem Recognition:

1. India is yet to recognise cyber-enabled human trafficking as a serious concern and take measures to counter the same.
2. Many countries globally recognised this pattern, which enabled them to act earlier, work in a coordinated manner helping them to take proactive legal action, and create policy measures to combat some forms of CEHT.
3. Emerging CEHT cases indicate that poverty and economic vulnerability are not the only precursors to human trafficking. Cyber technology has acted as an equaliser, making anyone who is emotionally vulnerable from any economic strata of society and using cyber technology in their daily life, a potential victim.
4. The perception that CEHT thrived only on the dark web is a myth. This is because traffickers have effortlessly committed their crimes on the surface web through popular social media platforms, matrimonial sites, dating sites, pages offering employment, etc.
5. Though the law enforcement authorities have observed the role of cyber technology in human trafficking during their everyday policing, their understanding of CEHT and its role is relatively nascent.
6. The lack of a definition for CEHT has led to fragmented and inadequate legal responses that fail to address the gravity and extent of the crime.

B. Newer Trends and Patterns :

7. Despite concerted efforts, traditional forms of human trafficking like commercial sexual exploitation, labour exploitation, organ trade, and illegal adoption continue unabated. To make matters worse, the use of cyber technology, which powers social media, job sites, dating sites, matrimonial sites, and instant messaging apps, has accelerated these existing crimes and have also led to the emergence of newer forms of the crime that target almost everyone who has access to cyber technology.
8. Young men from India who are either working in the Middle East in menial jobs or have just come back from the Gulf region, are being lured by the use of YouTube videos and social media groups to work in countries like Russia. They have been promised high paying jobs in the service industry and housekeeping, and even possibilities of living in Finland or other European nations. Instead, several of them have ended up working in active combat zones, risking their lives and liberties.

9. Young educated men who are computer literate and aspire for jobs abroad, are being lured using social media groups and job sites for high paying jobs in Thailand and Singapore, manipulated by fraudulent means and taken to the Golden Triangle of Laos, Cambodia, and Myanmar and kept in captivity and coerced to commit cyber-crimes.
10. The number of cyber-criminals who are themselves victims of human trafficking is increasing as cyber-scamming centres and compounds in several parts of South Asia expand and function with impunity.
11. Child trafficking for Child Sexual Abuse Material (CSAM) is on the rise with many technological applications, such as Telegram, providing an enabling platform on the surface web for such content to be bought and sold.
12. Online gaming apps are being used to groom and coerce children to self-generate sexually abusive material or work in the flesh trade industry.
13. The penetration of CEHT into financial crimes using methods such as fake loan apps, pig butchering, 'honey trapping,' sextortion, and 'package fraud,' is increasing the number of people vulnerable to being duped, trafficked, and forced to commit crimes and become traffickers.

C. Technology as a Key Enabler

14. Communication platforms such as WhatsApp, Telegram, and Facebook Messenger serve as primary channels for recruitment, transportation, and coordination for harbouring victims. Social media platforms such as Facebook, Instagram, dating sites, and online gaming applications serve as virtual hunting grounds for traffickers.
15. End-to-end encryption, self-destructing messages, and the lack of content moderation offered by the platforms are enabling human traffickers to commit crimes with anonymity and ease.
16. Digital currency transactions, seamlessly woven into the transactions of the traffickers, is allowing them to remain anonymous and make payments without any hassles.

D. Preparedness of Law Enforcement Officers

17. Human trafficking cases are handled through the AHTUs across the country. In many jurisdictions these AHTUs are not designated police stations, thereby lacking the powers to investigate any human trafficking crime, including those enabled by technology. Their role is limited to crime detection and rescue of victims, and thereafter the case is transferred to the local police station, which is not equipped to handle such cases since they require specialised investigation skills. All technology related crimes are investigated by Cyber Crime Police Stations. Consequently, the technology aspect in CEHT cases is not investigated by the law enforcement.
18. Law enforcement officers lack adequate technical skills, expertise, resources, and infrastructure to collect information for preventing early crime detection and intervention in CEHT cases.
19. The newer reporting mechanisms like cyber tip-lines/ cyber-crime portals have expanded the scope of reporting/detection of cases, but police officers are still largely dependent on traditional reporting methods, such as complaints by victims or their families and tip-offs from anonymous sources or concerned citizens.
20. Cyber forensics, collection and preservation of digital data, and meaningful interpretation of the data for effective prosecution of human trafficking cases, faces serious challenges in the uniform understanding of the preservation of digital evidence.
21. Lack of intra-state, inter-state, and international mechanisms to investigate human trafficking cases, especially those enabled by technology, has put law enforcers at a disadvantage while handling such cases.

E. Victim Services

22. The statutory support system offers support to victims who are women and children and leaves out men who are increasingly visible in CEHT cases.
23. Many victims of CEHT do not get access to formal support since they are treated as perpetrators of crime, ignoring the fact that their acts were committed under coercion.
24. Psycho-social interventions across the country do not factor in the digital damage on a victim while dealing with a case of CEHT.

25. Victims of newer forms of CEHT cases such as online criminality and recruitment for war zones are not entitled to any kind of services.

F. Accountability of Intermediaries

26. Most technology companies do not take proactive corrective action under the guise of privacy and freedom of speech/expression.
27. Their architecture does not have screening processes, and their products end up providing an enabling environment for traffickers.
28. Law enforcement officers find it challenging to get co-operation during investigation.
29. Some technology firms have started to recognise CEHT as a threat and have begun investing resources to develop technological solutions to counter the same. However, such actions are not part of their core business plan but mostly come under CSR initiatives, indicating perhaps a prioritisation of business interests over the prevention of crime.

G. Civil Society Organisations

30. Most civil society organisations working on anti-human trafficking acknowledge the increasing visibility of technology in all human trafficking cases. Some are supporting technological firms to improve safeguarding protocols by taking the role of 'trusted flaggers.'
31. A small number of organisations have filed cases to hold technological firms accountable in human trafficking cases.
32. A few organisations have effectively used technological solutions to detect and report human trafficking cases especially those related to child trafficking and child sexual abusive material.

II. Need for a National Plan of Action

The escalating nature of CEHT as revealed in the National Action Research Report demands an urgent and structured response. The crime is expanding exponentially, leveraging the anonymity and reach provided by cyber technologies to exploit vulnerable individuals. Currently, our preparedness to combat this sophisticated and pervasive crime is inadequate and the following concerns emerge from the research:

1. Growing anonymity of trafficking networks.
2. Rapid expansion targeting a larger population, with efforts to combat the crime still in its nascent stage.
3. Increasing digital penetration, heightening the vulnerability of children.
4. The urgent need to conceptualise CEHT within an effective legal framework and sensitisation of the criminal justice system towards the risks that a diverse socio-economic strata (including boys and men) face.
5. The widespread ease of production and dissemination of CSAM involving trafficked children on the surface web.
6. Generation of revenue at all levels of human trafficking, functioning beyond geographical boundaries, effortless integration of technology, and use of advanced technologies.
7. A scenario where there has been a crossover of the trafficked to the trafficker resulting in a large number of trafficked persons being compelled to act as perpetrators. The victim is physically and digitally exploited, while simultaneously being made to generate revenue for the traffickers
8. Lack of accountability among intermediaries.
9. While cybercrimes are increasingly recognized as a grave concern, the involvement of human trafficking networks behind them remains largely unacknowledged.

The draft NPoA aims to provide a comprehensive framework and blueprint to address the above- mentioned concerns and to equip the country in effectively addressing CEHT.

The national and global nature of CEHT necessitates a cohesive framework that can address both local and international dimensions of the crisis. This draft NPoA provides such a framework, structured to tackle the multifaceted challenges of CEHT. It aims to outline clear actions and strategies to prevent, detect, investigate, and prosecute these crimes while offering protection and support to victims.

III. Process Adopted for drafting NPoA

For the purposes of drafting this plan of action, the following definition has been used, which is in conformance with the definition of human trafficking provided both in the national laws and by United Nations Convention against Transnational Organized Crime (UNOTC), integrating the dimension of cyber technology:

“Cyber-Enabled Human Trafficking (CEHT) encompasses the use of digital technologies and online platforms for the recruitment, transportation, transfer, harbouring, or receipt of persons, by means of threat or use of force or other forms of coercion, abduction, fraud, deception, abuse of power or a position of vulnerability, or the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for exploitation, including sexual exploitation, forced labour, organ trafficking, and other forms of servitude.”

The findings of the action research and the inputs received from global experts, police officers who contributed to the data collection, and experts from civil society were used to prepare the first draft of the NPoA.

This draft was then circulated among 120 police officers, directors of judicial academies, directors of prosecution, women and child welfare officers, and civil society organisations from 27 states during a National Consultation on Countering ‘Cyber-Enabled Human Trafficking’ organised in collaboration with the Government of Andhra Pradesh at Vijayawada. Inputs from all the stakeholders were diligently integrated into the original draft.

The finalised draft National Plan of Action to Combat Cyber-Enabled Human Trafficking is a culmination of collective efforts and input gathered from all stakeholders from across the country, both within the criminal justice system and the welfare programs.

IV. Guiding Principles

Any national plan envisages a set of guiding principles that are non-negotiable, and which act as a doctrine to develop all strategies and interventions. As CEHT affects all persons alike in unique ways, leaving irreversible scars in the lives of human beings impacted, the following guiding principles will steer the NPoA.

❖ **Rights Based :**

The plan will be trauma-informed² and will ensure that the basic human rights of the victim are upheld and respected. Additionally, the following rights will be an integral part of each intervention:

• Right to dignity
• Right not to be re-traumatised and re-victimised
• Right to informed choices, privacy, and confidentiality
• Right to self-determination and participation

❖ **Individualised and Comprehensive :**

It will be inclusive and be able to address the needs of individuals and communities across all demographic regions.

❖ **Equitable :**

The plan will ensure that all services are accessible to all the regions. The activities are designed in a manner that facilitates people who may be facing more vulnerability or impact to have equal access to services.

❖ **Child Friendly & Gender-sensitive :**

The plan will be age-appropriate, child friendly, and recognise the gender-based vulnerabilities and risks.

❖ **Transparent & Accountable :**

The plan will be accountable and subject to mandatory external standardised social audit processes.

² For the purposes of this plan of action “trauma informed” means to recognise the trauma faced by the trafficked, and being mindful of personal and societal consequences, anticipating survivors’ response post trauma, and ensuring that all further action taken does not add to their trauma. The underlying principle is to foster growth, resiliency, and healing. (drawn from “What does it mean to be trauma-informed?”, Katherine King, Psy.D, www.psychologytoday.com)

V. Objectives

1. **Preventing Exploitation** : Educate vulnerable populations and the general public about the risks of CEHT and promote safe online practices.
2. **Enhancing Detection and Rescue** : Develop and deploy technological solutions to identify and assist victims swiftly.
3. **Care, Protection, Rehabilitation & Restitution**: Provide comprehensive care, protection, rehabilitation and restitution to CEHT survivors, ensuring their successful reintegration into society.
4. **Strengthening Legal Frameworks** : Update and enforce laws to address the unique challenges posed by CEHT.
5. **Capacity Building of stakeholders** : Strengthen the skills and knowledge of both state and non-state stakeholders to effectively combat CEHT.
6. **Fostering Collaboration** : Encourage cooperation among government agencies, law enforcement, technology companies, civil society organisations, and international partners.
7. **Robust Monitoring mechanisms** : Establish comprehensive monitoring systems to track and evaluate CEHT activities, ensuring timely detection, intervention, and accountability across all stakeholders.

VI. Structure and Flow of the National Plan of Action (NPoA)

The draft NPoA is structured to provide a comprehensive and systematic approach to combat CEHT. Each category within the NPoA addresses critical aspects of this issue and outlines specific measures to be implemented.

The proposed NPoA is structured as follows:

1. Institutional Framework
2. Prevention
3. Crime Detection
4. Investigation
5. Prosecution
6. Victim Protection
7. Legal Reforms
8. Capacity Building
9. Monitoring Mechanism

Each segment of the action plan is designed to cover specific activities and actions, ensuring a coordinated and comprehensive approach to combat CEHT. This structured flow not only enhances our national capabilities but also aligns with global efforts to tackle this critical issue effectively.

1. Institutional Framework

Establish an overarching institutional infrastructure and ecosystem for the effective prevention, detection, investigation, protection and prosecution of CEHT crimes, both nationally and internationally, in a coordinated and comprehensive manner.

1.1 Inter-Ministerial Coordination Council (IMCC):

Set up an inter-ministerial coordination council at the national level to act as the national advisory council that facilitates coordination among all relevant ministries. This council will be co-chaired by the Ministry of Home Affairs and the Ministry of Women and Child Development, with the Ministry of Electronics & Information Technology serving as the convenor. IMCC will also include four representatives from civil society who are domain experts in human trafficking and cybersafety. IMCC will meet twice a year.

1.2 National Coordination Centre (NCC) :

The Indian Cyber Crime Coordination Centre (I4C), in collaboration with Anti-Human Trafficking Unit (AHTU) cell of the Ministry of Home Affairs and a nodal unit set up by the Ministry of Electronics and Information Technology, would serve as the nodal centre, complete with a dedicated nodal officer and sufficient personnel, to oversee, coordinate, implement, and monitor the NPoA.

The National Coordination Centre (NCC) will maintain a panel of domain experts on human trafficking and cyber-safety from the civil society who will provide assistance as and when required.

The role of NCC, among others will include : -

- 1.2.1** Developing Standard Operating Procedures (SOPs) for inter-state cooperation and international law enforcement linkages including cooperation with Interpol to identify, investigate, and prosecute cases of CEHT, while strengthening the capacity of law enforcement agencies to effectively implement these procedures.
- 1.2.2** Recommending a regulatory and enforcement framework for securing cooperation from technology platforms and to hold them accountable for their role in the use of cyber technologies that recruit, control, and exploit victims.
- 1.2.3** Establishing mandatory minimum protocol for technology firms and intermediaries operating within the country, along with the appointment of an easily accessible nodal officer.
- 1.2.4** Establishing a national observatory to monitor CEHT cases, enhance data collection, and research the scope and nature of cyber technology misuse in order to develop solutions with nationwide application.

- 1.2.5** Coordinate with cybersecurity firms to gather intelligence on CEHT, with oversight provided by law enforcement agencies.
- 1.2.6** Recommending legislative reforms that strengthen legal provisions, enhance victim-centric justice delivery, and establish integrated victim support centres and compensation schemes for CEHT victims.
- 1.2.7** Facilitating training and capacity-building programs for law enforcement agencies, frontline workers, and legal professionals to improve their capabilities in detecting, investigating, and assisting victims of CEHT.

1.3. State Coordination Centre (SCC) :

Each state will establish a State Coordination Centre (SCC), chaired by the Chief Secretary and reviewed monthly. The SCC will be composed of senior police officers responsible for dealing with human trafficking and cybercrime cases, cyber safety experts, representatives from department of women and child welfare, representatives of all relevant line departments, and two credible civil society organisations working on the issue of human trafficking and cyber safety.

The SCC will be fully staffed and housed within the state's cybersecurity bureau/cyber dome/ cybercrime coordination centre, or its equivalent. With a designated department and a nodal officer, the SCC will manage and oversee efforts to combat CEHT both within and across states.

The National Coordination Centre (NCC) will fund the SCC and provide the necessary training to ensure effective execution of its role in addressing CEHT.

1.4 District Monitoring Cell (DMC) :

The District Monitoring Cell (DMC) will be established with full-time staff drawn from anti-human trafficking units, cyber-police stations, and civil society organisations working on human trafficking or cyber safety. It will be chaired by the District Collector/Magistrate, with the Superintendent of Police (SP) serving as the convenor.

The DMC, located at the SP's office, will oversee all CEHT cases within the district, ensuring adherence to proper case management protocols throughout the legal process and monitoring prevention campaigns. The DMC will report directly to the SCC and ensure that monthly data from the district is submitted.

1.5 Panchayat-Level Committees (PLC) :

One Anti-Human Trafficking Unit in every Panchayat will be designated as the Panchayat-Level Committee (PLC) to serve as the grassroot unit for reporting and addressing CEHT cases.

These cells will work closely with other police units and grassroots civil society organisations for local intelligence gathering, early detection of CEHT cases, establishing community reporting mechanisms for citizens to report confidentially, and undertaking community campaigns.

The PLC will send weekly reports to the District Monitoring Cell (DMC) on the cases prevented, detected, and prosecuted. The PLC will also report on the community-level campaigns conducted every month and its outreach efforts.

Stakeholders

Ministry of Home Affairs (MHA)
Ministry of Women & Child Development (MWCD)
Ministry of External Affairs (MEA)
Ministry of Electronics & Information Technology (MeitY)
Ministry of Information and Broadcasting (I & B)
Ministry of Labour and Employment (MOL&E)
Ministry of Overseas Indian Affairs (MOIA)
Ministry of Social Justice and Empowerment (MSJE)
Indian Cyber Crime Coordination Centre (I4C)
Ministry of Law & Justice (MoL& J)
Ministry of Rural Development (MoRD)
Ministry of Health and Family Welfare (MoHFW)
Ministry of Education (MoE)
State Governments represented by all line departments

2. Prevention

Efforts to prevent CEHT is possible by addressing the root causes of CEHT and by promoting awareness, reducing vulnerabilities, and building resilience within communities. A multi-stakeholder approach is necessary, bringing together government agencies, CSOs, the private sector, and technology platforms to implement targeted interventions. Digital literacy programs, public campaigns, and early warning systems can empower at-risk populations. Additionally, frameworks for regulating online spaces and technology use are essential for preventing exploitation and recruitment through digital platforms.

The National Coordination Centre (NCC) will :

- 2.1** Develop user-friendly age-appropriate training manuals on online safety and the dangers and signs of CEHT. It will pass necessary orders to integrate them into the curriculum of prominent education boards in India such as the Central Board of Secondary Education (CBSE); Indian Certificate of Secondary Education (ICSE); Council for the Indian School Certificate Examination (CISCE), National Institute of Open Schooling (NIOS); along with the equivalent various state boards to build awareness amongst children and young adults in educational setups (schools, colleges, vocational schools etc.)
- 2.2** Prepare training manuals to conduct community-based prevention programmes for raising awareness about CEHT and promote safe online practices for all frontline workers, including village volunteers of Panchayat Raj Institutions (PRI), District Rural Development Agency (DRDA), ASHA workers, Anganwadi workers, beat police officers, paralegal workers, anti-human trafficking clubs, and Cyber Volunteer. It will issue necessary directions to appropriate ministries to ensure the implementation of these manuals.
- 2.3** Develop audio-visual and other communication tools on online safety to be integrated across all ministries.
- 2.4** Forge partnerships with media organisations to produce and broadcast Public Service Announcements (PSAs) addressing the risks of CEHT, create reporting mechanisms, and disseminate information regarding the available support services through cinema theatres, television, and radio.
- 2.5** Develop mobile applications and online tools for all SCC that provide real-time assistance and resources for reporting suspicious online activities, malicious links, fake websites, and accessing support services.
- 2.6** Evolve safeguarding protocols on Government websites and earmark resources to unmask and blacklist fraudulent websites and spread awareness among job seekers on necessary due diligence.

- 2.7** Collaborate with technology companies and cybersecurity firms to implement measures such as age verification tools, content moderation algorithms, and reporting mechanisms to prevent online trafficking.
- 2.8** Create a database of free online safety tools and maintain a central repository of blacklisted sites and platforms that is accessible to law enforcement agencies, civil society, and the public.
- 2.9** Evolve upgraded parental control software and monitoring tools for all SCC that allow parents to supervise their minor children's online activities and protect them from potential risks.
- 2.10** Evolve safety control tools which can be purchased at their respective SCC by all establishments that provide public access to cyber technologies such as cyber cafes, schools and institutions having computer labs etc.
- 2.11** Establish robust digital mechanisms and accountability framework to monitor social media platforms, dark web applications, Play Store, App Store, EdTech store, and any other platforms on content moderation and compliance with existing laws.
- 2.12** Establish updated data analytics to identify trends and hotspots related to CEHT across the nation.
- 2.13** Develop prevention tools and mandatory reporting mechanisms of suspicious transactions.
- 2.14** Evolve strict regulatory provisions to be mandated to all financial institutions for usage of bank accounts with fake credentials.
- 2.15** Evolve regulatory mechanisms for the present Know Your Customer (KYC) procedures to address issues like "mule SIM cards" and "mule bank accounts". KYC procedures should extend to the usage of technical services too. Anonymous usage of these services should be prohibited.
- 2.16** Recommend Reserve Bank of India (RBI) to pass necessary directions to all financial institutions to adopt the preventive tools, mandatory reporting and regulatory mechanisms.

The State Coordination Centre (SCC) will :

- 2.17** Coordinate the adaptation and integration of user-friendly, age-appropriate training manuals on online safety and CEHT into state education board curricula including translation to local language.

- 2.18** Oversee the implementation of community-based prevention programs in the state by frontline workers.
- 2.19** Adapt audio-visual and communication tools on online safety in local language and facilitate the dissemination across all line departments in the state.
- 2.20** Collaborate with media organisations to produce and broadcast state specific PSAs addressing CEHT risks and available support services.
- 2.21** Monitor the implementation of safety control tools in public establishments, such as cyber cafes and schools.
- 2.22** Direct DMCs to gather data and identify trends related to CEHT within the state.

The District Monitoring Cell (DMC) will :

- 2.23** Oversee the implementation of community-based prevention programs by PLCs aimed at raising awareness about CEHT within the district.
- 2.24** Implement age-appropriate training programs in all educational institutions including coaching centres to raise awareness about online safety and the dangers and signs of CEHT based on manuals provided.
- 2.25** Gather monthly data from the PLCs on prevention efforts and community engagement activities and analyse trends to inform for strategic responses.
- 2.26** Provide regular reports to the SCC on the status of community initiatives and the effectiveness of training programs, highlighting areas for improvement and resource needs.
- 2.27** Organise training sessions for frontline workers in the district to equip them with the skills to recognize signs of CEHT and promote safe online practices.
- 2.28** Facilitate district-wide awareness campaigns on CEHT and online safety using audio-visual tools and resources.
- 2.29** Assess the effectiveness of community-based prevention programs and training initiatives, making necessary adjustments based on feedback and emerging trends in CEHT.
- 2.30** Distribute resources, tools, and support services for reporting suspicious activities to local stakeholders, including civil society organisations and community leaders.
- 2.31** Facilitate the establishment of confidential reporting mechanisms within the community, ensuring safety and support to any person when reporting suspicious activities.

The Panchayat-Level Committees (PLC) will :

- 2.32** Conduct community-based prevention programs focused on raising awareness about CEHT and promoting safe online practices among all communities through the frontline workers.
- 2.33** Ensure local media organisations broadcast PSAs that communicate the risks of CEHT, reporting mechanisms, and available support services to the community.
- 2.34** Encourage communities to use mobile applications and online tools for reporting suspicious online activities and accessing support services.
- 2.35** Inform the community about the safeguarding protocols established for government websites and promote awareness of due diligence practices among job seekers regarding fraudulent websites.
- 2.36** Educate parents on the importance and usage of parental control software and monitoring tools to supervise their children's online activities effectively.
- 2.37** Promote the use of safety control tools in public establishments, such as cyber cafes and educational institutions in the panchayat, ensuring that these measures are adopted for better online safety.
- 2.38** Track and report local trends and suspicious activities related to CEHT to the DMC for improved data analytics and strategic responses.

Stakeholders

Ministry of Education (MoE)
State Education Departments
I4C
University Grants Commission (UGC)
All India Council for Technical Education (AICTE)
Central Board of Secondary Education (CBSE)

Indian Certificate of Secondary Education (ICSE)
Council for the Indian School Certificate Examination (CISCE)
National Institute of Open Schooling (NIOS)
National Council of Educational Research and Training (NCERT)
State Councils of Educational Research and Training (SCERT)
Sarva Shiksha Abhiyan (SSA)
Ministry of Skill Development and Entrepreneurship (MSDE)
Ministry of Youth Affairs and Sports
National Skill Development Corporation (NSDC)
Ministry of Health and Family Welfare (MoHFW)
Ministry of Rural Development (MoRD)
Ministry of Women and Child Development (MWCD)
National Legal Services Authority (NALSA)
Nehru Yuva Kendra
Civil Society Organizations
National Social Service Scheme (NSS)
Registered Religious Legal Entities
Ministry of Information and Broadcasting (I&B)
Department of Information and Public Relations of States
Ministry of Electronics and Information Technology (MeitY)
Ministry of Labour & Employment (MoL&E)
Ministry of Finance
Reserve Bank of India (RBI)
Securities and Exchange Board of India (SEBI)

3. Crime Detection

Effective detection of CEHT cases requires a multi-layered approach that integrates advanced data analytics, intelligence sharing, and monitoring systems to proactively identify emerging threats. Collaboration between law enforcement, technology firms, and civil society is essential for real-time threat detection and early intervention. A unified national framework for information exchange will enhance inter-state coordination and cross-border detection efforts.

The National Coordination Centre (NCC) will:

- 3.1** Establish mandatory reporting mechanisms for all technological firms to report crimes related to CEHT and CSAM to the national nodal centre established by the NCC.
- 3.2** Recommend necessary amendments to the law which will ensure compliance regarding mandatory reporting.
- 3.3** Direct the National Cyber-Crime Research & Innovation Centre (NCR&IC), a wing of I4C, to develop advanced research tools, methodologies, and the use of OSINT and AI technologies for detecting CEHT cases, which will be made available to the SCC.
- 3.4** Create a centralised repository of CEHT investigative resources accessible to law enforcement agencies, allowing access to knowledge on emerging trends in offenders' modus operandi and up-to-date information on the fast-changing patterns of technology use and the technological landscape.
- 3.5** Empower law enforcement agencies to implement data analytics tools to monitor and analyse internet traffic in real-time for potential CEHT indicators.
- 3.6** In collaboration with technology companies, research institutions, and academic institutions, develop and deploy AI-powered detection systems utilising information from OSINT resources to identify and flag suspicious online activities related to human trafficking.
- 3.7** Develop protocols for the utilisation of the Inter-Operable Criminal Justice System (ICJS) and the Pariman Geo-Portal, developed by the National Informatics Centre (NIC), for anti-human trafficking efforts, and recommend adoption by states.
- 3.8** Review and strengthen the National Cyber-Crime Reporting Portal by I4C to include specific sections and features for reporting CEHT activities anonymously, ensuring ease of access and use for the general public.
- 3.9** Establish protocols and guidelines for information sharing on suspected CEHT cases and criminal networks between international agencies such as the

European Union Agency for Law Enforcement Cooperation (Europol) and the International Criminal Police Organisation (Interpol).

The State Coordination Centre (SCC) will :

- 3.10** Strengthen cyber patrolling tools to proactively identify online CEHT networks, with options for anonymous reporting.
- 3.11** Profile criminals and potential criminals through repository databases, including facial recognition and other biometric tools, available to law enforcement agencies.
- 3.12** Facilitate access for all DMC the centralised repository of CEHT investigative resources for law enforcement agencies, ensuring they are equipped with knowledge on emerging trends in offenders' modus operandi and technology use.
- 3.13** Oversee the use of data analytics tools by local law enforcement agencies to monitor and analyse internet traffic for potential indicators of CEHT.
- 3.14** Implement and recommend protocols for the use of the ICJS and the Pariman Geo-Portal in anti-human trafficking efforts at the state level.
- 3.15** Promote the use of National Cyber-Crime Reporting Portal for reporting CEHT activities anonymously in the state.
- 3.16** Provide information to NCC on suspected CEHT cases and criminal networks which have international linkages for effective case management of transnational human trafficking cases which are technology enabled.
- 3.17** Establish guidelines for information sharing on suspected CEHT cases and criminal networks with local law enforcement and community stakeholders, enhancing coordination and response efforts.
- 3.18** Provide training content to all DMCs on CEHT crime detection tools and monitor the implementation.

The District Monitoring Cell (DMC) will:

- 3.19** Provide regular training and refresher courses to all PLCs in the use of CEHT crime detection tools and monitor the usage of these tools.
- 3.20** Monitor data analytics tools and analyse internet traffic in real-time, identifying potential indicators of CEHT within the district.
- 3.21** Monitor the use of the National Cyber-Crime Reporting Portal in the district to

facilitate anonymous reporting of CEHT activities within the community, ensuring ease of access and encouraging local participation.

- 3.22** Inform and coordinate with SCC any CEHT case detected that has intra-state, inter-state or international implications from the district.
- 3.23** Report monthly to the SCC on the status of CEHT cases, investigative efforts, and any emerging trends in the district.

The Panchayat-Level Committees (PLC) will:

- 3.24** Encourage reporting suspicious online activities by the community and proactively register cases of CEHT through community reporting.
- 3.25** Provide information on anonymous reporting options for communities and ensure protection to whistle-blowers.
- 3.26** Collect and share data on local trends and suspicious activities related to CEHT with the DMC for improved data analytics efforts.
- 3.27** Organise regular workshops and training sessions for community members identified as trusted flaggers for the purpose of early crime detection.

Stakeholders

MHA
National Informatics Centre (NIC)
Ministry of Human Resource Development
MeitY
Indian Computer Emergency Response Team (CERT-In)
National Crime Records Bureau (NCRB)
Central Bureau of Investigation (CBI)
National Investigation Agency (NIA)
National Cyber-Crime Research & Innovation Centre (NCR&IC)
Telecom Regulatory Authority of India

4. Investigation

A well-structured investigative framework must leverage specialised cyber forensic tools, cross-sector collaboration, and streamlined protocols to track and dismantle trafficking networks. Inter-agency coordination, both domestic and international, is critical for timely access to evidence and resources. Building investigative expertise through continuous training, especially in digital forensics, will improve the ability to handle complex CEHT cases effectively.

The National Coordination Centre (NCC) will:

- 4.1** Develop protocols and issue advisories on all safeguarding measures, investigation, collection of evidence, and intra-state and inter-state cooperation mechanisms for time-bound investigation of CEHT cases within the country.
- 4.2** Initiate investigation of international/transnational nature of CEHT cases through pan-India investigating agencies and the international liaison focal point.
- 4.3** Make recommendations to the IMCC on regional cooperation mechanisms to enhance coordination and facilitate joint investigations into transnational criminal networks, necessitating multi-stakeholder collaboration with a victim-centric approach.
- 4.4** Develop advanced investigation tools in collaboration with licensed and accredited expert technological groups, which should be reviewed annually.
- 4.5** Develop and issue SOPs on seizure/ collection, custody/handling, analysing and preserving of digital evidence including following certification processes to present evidence in courts.
- 4.6** In consultation with the Reserve Bank of India (RBI), issue guidelines to banks and financial institutions to track and investigate financial transactions linked to CEHT activities in collaboration with the Financial Intelligence Unit-India (FIU-IND).
- 4.7** In collaboration with Telecom Regulatory Authority of India (TRAI), establish protocols for telecom companies to prioritise and promptly respond to law enforcement requests for data in CEHT investigations.

The State Coordination Centre (SCC) will:

- 4.8** Set up District-level anti-human trafficking police stations (DAHTU) with a special wing to investigate CEHT cases.
- 4.9** In consultation with NCC set up Joint Cyber Crime Coordination Teams (JCCT) for inter-state investigation of CEHT cases.
- 4.10** Facilitate intra-state investigation of CEHT cases.

- 4.11** Enhance digital forensic capabilities for evidence gathering, storage, and analysis by equipping CEHT units with advanced forensic tools and training, in collaboration with the National Forensic Sciences University and state forensic labs.
- 4.12** Establish adequate cyber forensic labs with advanced forensics resources, infrastructure and specialised manpower ensuring forensic reports are completed within two months, keeping up with the high volume of cases reported.

The District Monitoring Cell (DMC) will:

- 4.13** Implement through the DAHTU, SOPs for the collection, handling, and preservation of digital evidence in CEHT investigations as guided by the SCC.
- 4.14** Facilitate training sessions for law enforcement personnel within the district on advanced investigation techniques, digital evidence handling in collaboration with state forensic labs and procedures to seek information from technological firms.
- 4.15** Collect and analyse data related to CEHT cases in the district, ensuring timely submission of reports to the SCC for strategic oversight and resource allocation.
- 4.16** Develop a system for tracking the progress of CEHT investigations within the district, reporting any challenges or resource needs to the SCC.
- 4.17** Set up a district level panel of cyber security experts who will assist in complex CEHT cases.
- 4.18** In coordination with SCC undertake intra-state and inter-state investigation of CEHT cases.
- 4.19** Monitor case management of CEHT cases of DHTU and PLC on a day-to-day basis.

The Panchayat-Level Committees (PLC) will :

- 4.20** Undertake timely investigation of all the CEHT cases at the panchayat level.
- 4.21** Provide transparent tracking access to all complainants regarding the progress of the case.
- 4.22** Apply advanced technological tools to store and preserve digital evidence.
- 4.23** Seek support for cyber security experts from DMC in investigation of complex CEHT cases.

- 4.24** Maintain regular communication with the DMC to receive updates on investigation protocols, ensuring the PLC is equipped with current information and resources and is implementing it

Stakeholders

MHA
NCR&IC
National Forensic Sciences University (MFSU)
RBI
Financial Intelligence Unit-India (FIU-IND)
Telecom Regulatory Authority of India (TRAI)
Ministry of Finance
Cyber Expert Panel
Technological Firms

5. Prosecution

A victim-centred prosecution framework is essential for ensuring that offenders are held accountable without compromising on the well-being and safety of victims. Uniform legal processes across jurisdictions, expedited case management, and access to expert legal support will ensure fair and timely trials. While technology firms must also be legally compelled to cooperate with prosecution efforts, strengthening cross-border cooperation will address challenges posed by the transnational nature of CEHT.

The National Coordination Centre (NCC) will:

- 5.1** Make recommendations to states for setting up Additional Special Sessions courts with trained staff to expedite CEHT cases based on the volume of cases reported.
- 5.2** Make recommendations to the Ministry of Law & Justice to initiate amendments to existing laws in order to improve victim-centric justice delivery in CEHT cases.
- 5.3** Issue advisory for the appointment of trained Special Prosecutors.
- 5.4** Develop and issue comprehensive prosecutorial guidelines for CEHT cases to ensure consistent and effective legal strategies across jurisdictions.
- 5.5** Issue advisories on special provisions that need to be included in witness protection programs, tailored to risk assessments, to ensure the safety of individuals testifying in CEHT cases and their families. This should encompass secure housing, witness relocation, and identity protection as necessary.

The State Coordination Centre (SCC) will:

- 5.6** In consultation with the High Court, set up Additional Special Sessions Courts staffed by trained personnel with adequate infrastructure and advanced technology for presenting digital evidence in CEHT cases, in accordance with Section 173(3) of the BNS.
- 5.7** Make recommendations to the Director of Prosecution for the appointment of trained Special Prosecutors in courts dedicated to handling CEHT cases and presenting digital evidence.
- 5.8** Issue guidelines to establish a support system for witnesses and vulnerable-witness-friendly courtrooms, as per Section 180 of the BNS, including the designation of special counsellors to support victims and survivors during trials.
- 5.9** Establish robust case management systems to ensure delivery of justice within established time frames.

The District Monitoring Cell (DMC) will :

- 5.10** Support the establishment of Additional Special Sessions Courts within the district, ensuring that they are equipped with the necessary infrastructure and technology for presenting digital evidence in CEHT cases.
- 5.11** Assist in implementing guidelines for creating a supportive environment for witnesses and vulnerable-witness-friendly courtrooms, ensuring adherence to the provisions outlined in the BNS in collaboration with District Legal Services Authority (DLSA).
- 5.12** Monitor and report on the effectiveness of case management systems established for CEHT cases, ensuring timely delivery of justice and identifying areas for improvement.

The Panchayat-Level Committees (PLC) will:

- 5.13** Provide outreach support and legal aid through DLSA to all the complainants / victims for access to justice.
- 5.14** Collaborate with local law enforcement to facilitate witness support initiatives, ensuring community members are informed about available resources and assistance.
- 5.15** Encourage community members to report any issues or concerns related to the prosecution of CEHT cases, ensuring a feedback loop for continuous improvement.
- 5.16** Provide regular updates to the DMC on community engagement efforts related to witness support and the prosecution process for CEHT cases.

Stakeholders

MoL&J
MHA
National Legal Services Authority
State Government through the Law Department and Director of Prosecution
High Courts

6. Victim Protection

Comprehensive and uniform victim protection measures are critical to ensuring CEHT survivors' safety, recovery, and reintegration. Effective coordination between all stakeholders, both state and non-state, including law enforcement, health services, and CSOs, will enhance access to trauma-informed care and rehabilitation. Standardised protocols across jurisdictions will ensure consistency in victim identification, need based support, and access to legal and psychological support. CSOs play a key role in fostering trust and providing innovative solutions for long-term victim recovery and empowerment in CEHT cases.

The National Coordination Centre (NCC) will:

- 6.1** Recommend to the concerned ministries to introduce schemes for establishing "Integrated Victim Support Centres for CEHT Victims," with clearly defined standards of care for these centres, ensuring they are appropriately budgeted.
- 6.2** In consultation with the National Legal Services Authority, strengthen the existing victim compensation scheme to factor in the digital damage to the mental health of victims.
- 6.3** In consultation with the Ministry of Law and Justice, recommend necessary amendments to existing legislation to mandate that technology companies pay damages to victims as part of the restitution process.
- 6.4** Recommend a comprehensive victim-witness protection scheme, which includes provisions for identity changes, if necessary, safe accommodation for victims and their families until the trial concludes, and ensuring access to these services for victims who have been compelled to commit crimes.

The State Coordination Centre (SCC) will:

- 6.5** Direct concerned stakeholders to set up gender-neutral Integrated Victim Support Centres (IVSCs) in all districts, which will include a hotline and trauma-informed support services such as psycho-social care, medical care, specialised counselling, legal aid, and both institutional and non-institutional rehabilitation support. The rehabilitation package should encompass educational opportunities, skill development, job placements, a continuum of care, entrepreneurship training, and loans/grants for small and medium enterprises for victims.
- 6.6** In consultation with the Home Department and FRRO, direct stakeholders concerned to establish special cells within selected IVSCs for foreign victims, providing support services for repatriation or deportation.
- 6.7** Direct stakeholders concerned to implement victim-witness protection schemes

for CEHT victims and their families, which may include identity changes, if necessary, provisions for safe accommodation until the trial concludes, and ensuring access to these services for victims who have been compelled to commit crimes.

The District Monitoring Cell (DMC) will :

- 6.8** Facilitate the establishment of IVSCs at the district level, ensuring access to trauma-informed support services for victims of CEHT.
- 6.9** Monitor the effective implementation of hotline services within the IVSCs for immediate assistance to victims.
- 6.10** Facilitate training for personnel at the IVSCs to provide psycho-social care, medical care, specialised counselling, legal aid, and rehabilitation support for victims.
- 6.11** Collaborate with local educational institutions and vocational training centres to provide educational opportunities and skill development for victims as part of their rehabilitation.
- 6.12** Maintain communication with the SCC to report on the establishment and functioning of IVSCs, highlighting any challenges and resource needs.

The Panchayat-Level Committees (PLC) will :

- 6.13** Create awareness about the services provided by IVSCs in the community.
- 6.14** Complete threat perception assessment of victims and recommend to authorities concerned, including law enforcement agencies and courts for necessary action.
- 6.15** Assist community members in accessing resources related to victim support services, including the hotline and information about legal aid and rehabilitation programs.
- 6.16** Collect feedback from victims and their families regarding the effectiveness of support services offered at the IVSCs and report this information to the DMC for necessary action.
- 6.17** Facilitate local outreach programs to inform victims about their rights and available protections, ensuring they are aware of victim-witness protection schemes.
- 6.18** Establish community networks to provide safe accommodation for victims until they can access services, ensuring their safety and well-being during the recovery process.

Stakeholders

MHA
MWCD
MEA
State Social Welfare Departments
National Skill Development Corporation (NSDC)
MoHFW
MoHFW
MoRD
Ministry of Micro, Small and Medium Enterprises (MSME)
District Heads of Administration, Police, and Judiciary
Legal Services Authorities

7. Legal Reforms

There is a need for a comprehensive National Legal Framework that defines CEHT, encompassing all aspects of this crime, ensuring inter-state and international cooperation, providing holistic trauma-informed victim services, and holding technology firms accountable for their role as enablers. Amendments to existing laws are essential to ensure the use of technology for CEHT is treated as an aggravated form of crime.

The National Coordination Centre (NCC) will :

- 7.1** Recommend appropriate legal amendments to the Bhartiya Nyaya Sanhita (BNS), the Bharatiya Nagarik Suraksha Sanhita (BNSS), the Information Technology Act (IT Act), the Immoral Traffic (Prevention) Act (ITPA), the Juvenile Justice (Care and Protection of Children) Act, the Child Labour (Prohibition and Regulation) Act, the Commissions for Protection of Child Rights Act, and the Protection of Children from Sexual Offences Act (POCSO). These amendments will clarify the definitions of CEHT, data protection, data retention, penalties, technological firm liability, and enforcement mechanisms.
- 7.2** Draft comprehensive legislation through multi-stakeholder consultation to address CEHT and recommend it for adoption through the IMC.
- 7.3** Issue protocols and procedures for intelligence gathering, evidence collection, witness protection, victim protection, and handling foreign nationals in CEHT cases.
- 7.4** Develop detailed guidelines for legal safeguards on the ethical use of technology in detecting and prosecuting CEHT, ensuring civil liberties and privacy protections.
- 7.5** Recommend adoption of data retention policies by relevant ministries, requiring Internet Service Providers (ISPs) and telecom companies to retain user data for a specified period to aid CEHT crime investigations.

Stakeholders

MoL& J
MHA
MeitY
Internet Service Providers (ISPs)
Telecom companies

8. Capacity Building

Building the capacity of stakeholders is essential to ensure a swift and coordinated response to CEHT. Comprehensive training programs for law enforcement, judiciary, and frontline workers will help develop specialised skills in detection, investigation, and victim support. Fostering partnerships with academia, technology platforms, and CSOs will drive innovation, while regular audits and performance assessments will ensure sustained operational effectiveness.

The National Coordination Centre (NCC) will :

8.1 Develop comprehensive training resource materials, including SOPs and training manuals, for Law Enforcement Agencies (LEAs), prosecutors, judicial officers, relevant service providers, civil society organisations, legally competent bodies, labour officials, and financial institutions on:

- ❖ Enhancing capacity to detect CEHT cases and identify victims and perpetrators.
- ❖ Enhancing capacity to investigate and prosecute CEHT cases, including appreciation of digital evidence.
- ❖ Increasing capacity to provide victim-centred assistance to survivors.
- ❖ Enhancing capacity to prevent CEHT crimes.
- ❖ Improving documentation of CEHT cases.

8.2 Develop comprehensive training resource materials, including SOPs and training manuals for frontline workers, such as Anganwadi Workers, ASHA Workers, Village Volunteers, Panchayat Raj Institutions, educational institutions, airport staff, immigration officers etc., on:

- ❖ Dangers of CEHT.
- ❖ Identifying potential victims.
- ❖ Identifying perpetrators.
- ❖ Reporting mechanisms.

The State Coordination Centre (SCC) will :

8.3 In collaboration with the state police academy and judicial academy, conduct induction orientation, refresher training, and advanced training for all stakeholders in the criminal justice system on CEHT.

- 8.4** In collaboration with the state police academy, conduct specialised training for District Monitoring Cells, Panchayat-Level Committees, and all Anti-Human Trafficking Police Stations with special CEHT wings on the latest technologies, investigative techniques, state-of-the-art tools and technologies, ethical considerations in cyber-crime investigations, and procedures to request electronic evidence from private companies and obtain cooperation from other states or countries.
- 8.5** In collaboration with the state police academy, conduct specialised training for prosecutors on handling and presenting electronic evidence before a judge.
- 8.6** In collaboration with training agencies of different departments, organise capacity-building programs for frontline workers, CSOs, and first responders, focusing on strategies to preserve digital evidence, such as storing chat histories while assisting in crime detection.
- 8.7** In collaboration with the state judicial academy, conduct regular training for emerging lawyers on the complexities of CEHT cases, including digital evidence and cyber laws.
- 8.8** In collaboration with the state police academy, conduct training programs for certified expert witnesses in cyber-crime and human trafficking to provide credible testimony in court.

The District Monitoring Cell (DMC) will :

- 8.9** Coordinate with SCC to arrange district specific specialised training sessions for DMC personnel and Anti-Human Trafficking Police Stations, focusing on investigative techniques, ethical considerations, and procedures for requesting electronic evidence.
- 8.10** Ensure that training programs for prosecutors on handling and presenting electronic evidence are accessible to local legal practitioners, facilitating knowledge transfer within the district.
- 8.11** Work with PLCs to implement capacity-building programs for frontline workers, CSOs, and first responders on preserving digital evidence and effective strategies for crime detection.
- 8.12** Report to the SCC on the status of training initiatives and identify any gaps in knowledge or resources required to enhance capacity-building efforts within the district.

The Panchayat-Level Committees (PLC) will :

- 8.13** Implement capacity-building workshops for frontline workers and community members to enhance their understanding of CEHT, digital evidence preservation, and reporting mechanisms.

- 8.14** Work closely with the DMC to assess and address specific training needs of local volunteers and first responders, ensuring their roles in supporting CEHT victims are effectively supported.
- 8.15** Promote community engagement in training programs by disseminating information on the importance of preserving digital evidence and reporting suspicious activities related to CEHT.
- 8.16** Collect and analyse feedback from participants after training sessions to evaluate the effectiveness of the programs and share insights with the DMC for continuous improvement.

Stakeholders

MHA
National Judicial Academy (NJA)
State Judicial Academies
National Police Academy (NPA)
Bureau of Police Research and Development (BPR&D)
MWCD
MOL&E
MoHFW
Ministry of Civil Aviation (MoCA)
Indian Railways
I4C
Legal Services Authorities
State Judicial Academies
State Police Academies
Human Resource Development Institutions
State Training Institutions
Bar Council of India (BCI)

9. Monitoring Mechanism

To ensure the effective implementation of the NPoA, a robust monitoring mechanism will be established and integrated with the institutional framework. This will include clearly defined timelines for monitoring at various levels. A Monitoring, Evaluation, and Learning (MEL) framework will be incorporated to provide continuous oversight and facilitate ongoing improvement of CEHT prevention and response strategies. Regular impact assessments will support the process, providing critical insights for refining and updating guidelines and policies aimed at combating CEHT.

9.1 Reviews:

9.1.1 The Inter-Ministerial Coordination Council will conduct yearly reviews of the implementation of the NPoA.

9.1.2 The National Coordination Centre will conduct quarterly reviews of the functioning of all SCCs.

9.1.3 SCCs will conduct monthly reviews of all district-level activities through the DMC, and the reports will be sent to the National Coordination Centre.

9.1.4 DMCs will conduct fortnightly reviews of all PLCs, and the reports will be sent to the SCC.

9.2 Impact Assessment : An annual social audit will be conducted by an external agency to evaluate the implementation of the NPoA. The relevance, upgradation, and re-strategizing of the NPoA will occur every two years based on these assessments.

9.3 Transparency and Accountability : An annual "National Status Report on CEHT" will be presented to the nation, detailing accomplishments, gaps, challenges, and the way forward. This report will be uploaded to the ICJS portal to ensure transparency and accessibility.

Stakeholders

MHA
State Governments through the Home Department
Heads of District Administrations, Police, and Prosecutions
ICJS Portal

Annexure

LIST OF CONTRIBUTORS

Sl. No.	Name	State	Designation	Stakeholder
1	Shri. A. Hari Haranadha Sarma	Andhra Pradesh	Director, Judicial Academy	Judicial Officer
2	Smt. M. Krishnaveni	Andhra Pradesh	Prl. SA, AP Technology Services	IT Department
3	Shri. Bammidi Chandrashekhar Rao	Andhra Pradesh	Bachpan Bachao Andolan	Law Enforcer
4	Smt. KGV Saritha	Andhra Pradesh	SP, Women Protection Cell, CID	Law Enforcer
5	Smt. Krishna Prasanna	Andhra Pradesh	SP, Cyber Crimes	Law Enforcer
6	Sri. Ramakoteswar Rao	Andhra Pradesh	Director of Prosecution	Prosecutor
7	Sri. Ajoy Prem Kumar	Andhra Pradesh	Joint Director - Prosecution	Prosecutor
8	Sri. V Rajendra Prasad	Andhra Pradesh	Joint Director - Prosecution	Prosecutor
9	Shri M.A.Hameed	Andhra Pradesh	Public Prosecutor	Prosecutor
10	Shri Ram Babu	Andhra Pradesh	CI, AP Police	Law Enforcer
11	Shri Madhu Babu	Andhra Pradesh	CI, AP Police	Law Enforcer
12	Shri. G.P. Shireesha	Andhra Pradesh	CI, AP Police	Law Enforcer
13	Smt. P. Syamala Aparna	Andhra Pradesh	SI, AP Police	Law Enforcer
14	Shri Murthy	Andhra Pradesh	SI, AP Police	Law Enforcer
15	Shri Rambabu	Andhra Pradesh	SI, AP Police	Law Enforcer
16	Ms. Rajani	Andhra Pradesh	SI, AP Police	Law Enforcer
17	Ms. Varsha	Andhra Pradesh	SI, AP Police	Law Enforcer
18	Suma Sahiti	Andhra Pradesh	SI, AP Police	Law Enforcer
19	Shri G. Kennedy	Andhra Pradesh	CI, AP Police	Law Enforcer
20	Smt. Y Sailaja	Andhra Pradesh	Joint Director, WD&CW Dept	Women & Child Welfare Officer
21	E. Sree Rachana	Andhra Pradesh	SI, AP Police	Law Enforcer
22	Smt. Vijaya Sree	Andhra Pradesh	ACDPO, WD&CW Dept	Women & Child Welfare Officer

23	Shri Dinesh	Andhra Pradesh	Research Officer, WD&CW Dept	Women & Child Welfare Officer
24	Shri Krishna Prasad Das	Andhra Pradesh	SMC-SHEW, AP WCD	Women & Child Welfare Officer
25	Smt. Jayanthi	Andhra Pradesh	Gender Specialist, SHEW, AP WCD	Women & Child Welfare Officer
26	Ms. Anitha	Andhra Pradesh	Accounts Assistant, WD&CW Dept	Women & Child Welfare Officer
27	Shri Sudhakar Babu	Andhra Pradesh	Legal Counsellor, WD&CW Dept	Women & Child Welfare Officer
28	Smt. Anuradha	Andhra Pradesh	Social Counsellor, WD&CW Dept	Women & Child Welfare Officer
29	Smt. Uma Devi	Andhra Pradesh	DW&CW&EO, NTR	Women & Child Welfare Officer
30	Smt. Suvarna	Andhra Pradesh	DW&CW&EO, Krishna	Women & Child Welfare Officer
31	Shri P. Srinivas	Andhra Pradesh	Senior SE, APTS	IT Department
32	KVAS Vijayalakshmi	Andhra Pradesh	CDPO	Women & Child Welfare Officer
33	P.P.G Prasoon	Andhra Pradesh	CDPO	Women & Child Welfare Officer
34	Smt. E. Tulasi	Andhra Pradesh	WCD	Women & Child Welfare Officer
35	Smt. A. Padmavathi	Andhra Pradesh	WCD	Women & Child Welfare Officer
36	Smt. MDM Priyamka	Andhra Pradesh	WCD	Women & Child Welfare Officer
37	Smt. V Deepthi	Andhra Pradesh	ICDS Project	Women & Child Welfare Officer
38	Smt. M Lavanya	Andhra Pradesh	ICDS Project	Women & Child Welfare Officer
39	Smt.G. Udaya Lakshmi	Andhra Pradesh	ACDPO , AP WCD	Women & Child Welfare Officer
40	Smt. K. Simhachalam	Andhra Pradesh	ACDPO , AP WCD	Women & Child Welfare Officer
41	Smt. T.L. Sarawathi	Andhra Pradesh	CDPO	Women & Child Welfare Officer
42	Smt.T. Harathi	Andhra Pradesh	ACDPO ,AP WCD	Women & Child Welfare Officer
43	G. Satyavathi	Andhra Pradesh	CDPO	Women & Child Welfare Officer

44	Smt. A. Sridevi	Andhra Pradesh	CDPO, AP WCD	Women & Child Welfare Officer
45	L. Raja Varsh	Andhra Pradesh	SI, AP Police	Law Enforcer
46	T. Girija	Andhra Pradesh	ADD PSTO SEE, WCD	Women & Child Welfare Officer
47	Ch. Indira	Andhra Pradesh	CDPO	Women & Child Welfare Officer
48	N.Suneetha Devi	Andhra Pradesh	ACDPO, AP WCD	Women & Child Welfare Officer
49	Sri P. Somasankar	Andhra Pradesh	Supdt, WD&CW Dept	Women & Child Welfare Officer
50	Shri. A. Krishna Kumari	Andhra Pradesh	CDPO	Women & Child Welfare Officer
51	Mr. Chandra Sekhar	Andhra Pradesh	State Coordinator, Bachpan Bachao Andolan	Civil Society Organisation
52	Shri. L. Raja Varsh	Andhra Pradesh	SI, AP Police	Law Enforcer
53	Shri Dr. Venkatesh	Andhra Pradesh	Police	Law Enforcer
54	P. Soma Sankar	Andhra Pradesh	WCD	Women & Child Welfare Officer
55	CH. Laxmi Bai	Andhra Pradesh	WCD	Women & Child Welfare Officer
56	Venkateshwara Reddy	Andhra Pradesh	Cyber Security	IT Department
57	Shyam Sundar	Andhra Pradesh	Editor Hans India	Media
58	Ms. Shilpi Singh	Bihar	Director, Bhoomika Vihar	Civil Society Organisation
59	Shri Dharmbir Singh	Bihar	Joint Director, Department of Social Welfare	Civil Society Organisation
60	Dr. Gopal Arora	Chandigarh	Addl. District & Sessions Judge, Judicial Academy	Judicial Officer
61	Shri. Rajinder Singh	Chandigarh	District Attorney (Consumer Protection)	Prosecutor
62	Ms. Shipra Bansal	Chandigarh	Chairperson, Chandigarh Commission for Protection of Child Rights	Women & Child Welfare Officer
63	Shri. Abhay Dewangan	Chhattisgarh	Deputy Director, WCD	Women & Child Welfare Officer

64	Shri Sachitanand Mishra	Daman and Diu	State Mission Coordinator	Civil Society Organisation
65	Shri. Rajneesh Gupta	Delhi	IPS Jt. CP Special Cell	Law Enforcer
66	Smt. Rashmi Sharma Yadav	Delhi	DCP, I4C, MHA	Law Enforcer
67	Munesh Dutt	Delhi	Deputy Director, I4C, MHA	Law Enforcer
68	Naresh Kumar	Delhi	AC, I4C, MHA	Law Enforcer
69	Ms. Chitra Iyer	Delhi	Co-Founder and CEO, Space 2 Grow	Civil Society Organisation
70	Ms. Sakshi Mehra	Delhi	Associate	Civil Society Organisation
71	Ms. Swati Arora	Delhi	Project Manager, Cyber Peace Corps	Civil Society Organisation
72	Shri Ravi Kant	Delhi	Country Head-Access to Justice	Civil Society Organisation
73	Shri Sanjay Kumar Sain, IPS	Delhi	Deputy Commissioner of Police, Delhi	Law Enforcer
74	Shri Rajesh Kr. Singh	Delhi	Director, Delhi Judicial Academy	Judicial Officer
75	Sharon Thambala	Delhi	PTI	Media
76	Ms. Arnika Singh	Goa	Social Media Matters	Civil Society Organisation
77	Shri Amitabh Kumar	Goa	Social Media Matters	Civil Society Organisation
78	Dr. S.P. Rajkumar, IPS	Gujarat	ADGP CID, Crime & Railways	Law Enforcer
79	Shri. Dharmendra Sharma, IPS	Gujarat	SP, State Cyber Cell, CID Crime	Law Enforcer
80	Ms. Triveni Acharya	Gujarat	Rescue Foundation	Civil Society Organisation
81	Shri. B.M.T ank	Gujarat	Superintendent of Police, State Cyber Crime Cell	Law Enforcer
82	Smt. Manisha	Haryana	HPS DSP, State Crime Branch	Law Enforcer
83	Shri. Ashwani Bajaj	Haryana	District Attorney, Bhiwani	Prosecutor
84	Shri. Nishi Kant	Haryana	Shakti Vahini	Civil Society Organisation
85	Ms. Narayani Bhattacharya	Himachal Pradesh	STOP	Civil Society Organisation
86	Ms. Sonia Gupta	Jammu & Kashmir	Director, Judicial Academy	Judicial Officer

87	Shri. Mohinder Kumar	Jammu & Kashmir	District Nodal Officer, Cyber Jagrukta Diwas Ramban	Law Enforcer
88	Shri. Faisal Hussain	Jammu & Kashmir	Crime Branch, Srinagar, Kashmir	Law Enforcer
89	Shri. Manoj Prasad	Jharkhand	Director, Judicial Academy	Law Enforcer
90	Shri. Sanjay Kumar Mishra	Jharkhand	Secretary, Bal Kalyan Sangh	Civil Society Organisation
91	Smt. Pushpalatha G. Rayar	Karnataka	Joint Director (PDM)	Women & Child Welfare Officer
92	Smt. Anjali Devi	Karnataka	Director, Dept of Prosecution & Govt Litigation	Prosecutor
93	Smt. Madhumathi Nagaraja Sidnoorkara	Karnataka	Law Officer	Prosecutor
94	Ms. Sherlin Anthony	Karnataka	Vihaan	Civil Society Organisation
95	Smt. Rekha Abel	Karnataka	Prajwala	Civil Society Organisation
96	Ms. Jeebin Lolita Sain	Kerala	District WCD Officer	Women & Child Welfare Officer
97	Ms. Ajeetha Begum, IPS	Kerala	DIG Thiruvananthapuram Range, State Nodal Officer for Anti-Trafficking	Law Enforcer
98	Smt. Ann Thania Alex	Kerala	Assistant Director, Judicial Academy	Judicial Officer
99	Smt. Fareeda Majeed	Kerala	Director of Prosecution (Admn)	Prosecutor
100	Shri. Bramwell	Kerala	ICMEC	Women & Child Welfare Officer
101	Shri Prakash S.P	Kerala	Inspector of Police	Law Enforcer
102	Ms. Ajeetha Begum, IPS	Kerala	DIG Thiruvananthapuram Range, State Nodal Officer for Anti-Trafficking	Law Enforcer
103	Shri. Suresh Tomar	Madhya Pradesh	State Nodal Officer of Mission Shakti WCD	Civil Society Organisation
104	Shri. Sunil Gawande	Madhya Pradesh	NIWCYD Bachpan	Civil Society Organisation
105	Shri. Anil A. Gawade	Maharashtra	Director, Snehalaya	Civil Society Organisation

106	Ms. Jaya Jogdand	Maharashtra	President, Snehalaya	Civil Society Organisation
107	Ms. Naorem Ranjana Devi	Manipur	Diocesan Social Service Society	Civil Society Organisation
108	Shri. R Thangneisel Savio	Manipur	CRS	Civil Society Organisation
109	Shri. C.V.S. Reddy, IPS	Meghalaya	Dy IGP, CID, Shillong	Law Enforcer
110	Smt. Natalie Ion Dkhar	Meghalaya	Deputy Director, State Judicial Academy	Judicial Officer
111	Shri. D. Lyngdoh	Meghalaya	JS, Law Department	Judicial Officer
112	Shri. Anis Kharsohum	Meghalaya	Impulse NGO Network	Civil Society Organisation
113	Sr. Helen Liansangpuui	Mizoram	Zoram Entu Pawl	Civil Society Organisation
114	Prof. B. Govind Rao	Odisha	A.R.U.N.A	Civil Society Organisation
115	Shri Ritesh Kumar Mohapatra	Odisha	DSP , CID CB	Law Enforcer
116	Smt. Sarita Badgujar	Rajasthan	ASP-AHT	Law Enforcer
117	Rajpal Panwar	Rajasthan	Jansahas	Civil Society Organisation
118	Ms. Amu Vinzuda	Rajasthan	Jan Sahas Society	Civil Society Organisation
119	Shri Sunand Kumar Singh	Rajasthan	Bachpan Bachao Andolan	Civil Society Organisation
120	Shri G. Hari Kumar	Tamil Nadu	ADSP, Thiruvallur, TN	Law Enforcer
121	Smt. Meenakshi	Tamil Nadu	SP Cyber Crime Wing	Law Enforcer
122	Shri. G. Venkat Rao	Telangana	Inspector	Law Enforcer
123	Shri. K. Swetha	Telangana	CPDO, Women Development & Child Welfare	Women & Child Welfare Officer
124	Shri. P. Sreedhar	Telangana	DSP, WSP, Telangana	Law Enforcer
125	Shri. Mahesh M. Bhagwat, IPS	Telangana	IPS, ADGP , Law and Order	Law Enforcer
126	Shri. Phani Kumar	Telangana	Prosecutor	Prosecutor
127	Shri. Satyanarayana	Telangana	Prosecutor	Prosecutor
128	Dr. M. Suneetha	Telangana	SMC, SHEW, WD&CWD	Women & Child Welfare Officer
129	Smt. G. K. Sunandha	Telangana	JD, WD&CWD	Women & Child Welfare Officer
130	Shri. Divesh Chandra Samant	Uttar Pradesh	Director, JTRI	Judicial Officer

131	Shri. Rajesh Mani	Uttar Pradesh	Manav Seva Sansthan	Civil Society Organisation
132	Shri. Tushar Sharma	Uttar Pradesh	Cyber Security Researcher & Lawyer	Prosecutor
133	Shri. Harish Kumar Goel	Uttarakhand	Director, Uttarakhand Judicial Legal Academy	Judicial Officer
134	Smt. Glory Murthy	West Bengal	International Justice Mission	Civil Society Organisation

LIST OF CONTRIBUTORS-POLICE OFFICERS (DATA COLLECTION)

S.No.	Name	State	Designation
1	P. Arjamma	Andhra Pradesh	S.I. of Police, Disha P.S., Kakinada
2	D. Rajya Lakshmi	Andhra Pradesh	S.I. of Police, Disha P.S., Konaseema
3	V. Kanthipriya	Andhra Pradesh	S.I. of Police, Disha W.P.S., Eluru
4	Sk. Ameenabegum	Andhra Pradesh	S.I. of Police, Disha P.S.
5	T. Aruna Kumari	Andhra Pradesh	S.I. of Police, Kavali G.R.P., Guntakal Railway District
6	K. Vasavi	Andhra Pradesh	Inspector of Police, Disha P.S., I/C AHTU, Velaya
7	D. Sakuntala	Andhra Pradesh	S.I. of Police, Disha P.S., ASR District
8	T. Laskshmi	Andhra Pradesh	Inspector of Police, Disha P.S., Anakapalli
9	P. Syamali	Andhra Pradesh	S.I. of Police, Disha W.P.S., Vizianagaram
10	P. Syamala Aparna	Andhra Pradesh	S.I., CCPS, CIO
11	N. Gowri	Andhra Pradesh	S.I. of Police, Disha W.P.S.
12	B. Bhudevi	Andhra Pradesh	Women P.C.
13	T. Mahita	Andhra Pradesh	W.S.I., CID RO, Nellore
14	P. Fathima	Andhra Pradesh	S.I. of Police, CID RO, Guntur
15	D. Chandra Sekhar	Andhra Pradesh	Inspector of Police, CID, CCPS, HQPS
16	Ch. Venkateshwara Rao	Andhra Pradesh	Inspector of Police, CID RO, RJY
17	T. Bhadra Rao	Andhra Pradesh	S.I. of Police, CID RO, Vijayawada
18	S. Subba Raju	Andhra Pradesh	S.I. of Police, CID RO, Tirupati
19	M. Mohan	Andhra Pradesh	S.I., Cybercrimes, CID
20	S. Naseeruddin Peer	Andhra Pradesh	P.C., CID RO, Kurnool
21	B. Balakrishna	Andhra Pradesh	S.I., 30, Cybercell Rayachoti
22	A. Sunny Babu	Andhra Pradesh	P.C. 6016, CID RO, Guntur
23	V. Thulasiram	Andhra Pradesh	P.C. 4327, Disha W.P.S., Chittoor
24	R. SivakeSavulu	Andhra Pradesh	P.C. 2405, Disha W.P.S., Tirupati
25	K. Sarat Chandra	Andhra Pradesh	C.I. of Police, Disha P.S., Tirupati
26	K. Balaiah	Andhra Pradesh	Inspector of Police, Disha P.S., Chittoor

27	T. Ch. Govindu	Andhra Pradesh	Inspector of Police, Disha P.S., Anantapur
28	D. Mallikagida	Andhra Pradesh	Inspector of Police, Disha W.P.S., Ongole
29	K.Srinu	Andhra Pradesh	P.C. 2353, Disha W.P.S., Ongole
30	K. Kola Venkata Ramana	Andhra Pradesh	C.I., Disha W.P.S., Kurnool
31	G. Iqbal	Andhra Pradesh	S.I. of Police
32	K. Mallikarjuna Rao	Andhra Pradesh	P.C.
33	B.U. Mahesh	Andhra Pradesh	Constable
34	Y.Ch. Alluri Reddy	Andhra Pradesh	C.I. of Police
35	B. Siva Koteswara Rao	Andhra Pradesh	P.C. 6111
36	V. Subba Rao	Andhra Pradesh	S.I. of Police, Disha
37	S. Satish	Andhra Pradesh	P.C. 1422
38	Mottavi Krishna	Andhra Pradesh	P.C. 338, Disha, PVP (M)
39	B. Mohan Babu	Andhra Pradesh	P.C. 3718, Disha W.P.S., Kurnool
40	P.V. Ramana Murty	Andhra Pradesh	S.I., CID
41	K. Paidapu Naidu	Andhra Pradesh	C.I., CID
42	B. Supriya	Andhra Pradesh	C.I., CID RO, VSP
43	M. Sudhakara Rao	Andhra Pradesh	H.C. 106, CID RO, USP
44	P. Saroja	Andhra Pradesh	S.I. 146
45	K. Srinivasa Rao	Andhra Pradesh	S.I. of Police
46	K. Ravi Kiran	Andhra Pradesh	P.C.
47	R. Murali Mohan	Andhra Pradesh	S.I. of Police
48	D. Sathish Babu	Andhra Pradesh	A.S.I., AHTU, SPS Nellore
49	TVS. Ramababu	Andhra Pradesh	P.C. 420
50	G. Babi Rani	Andhra Pradesh	WAS- 699
51	JJN. Rao	Andhra Pradesh	P.C. 3611
52	M. Bala Krishna	Andhra Pradesh	P.C. 2136
53	M. Ramya	Andhra Pradesh	S.I.
54	K. Lalitha	Andhra Pradesh	Women H.C.

55	I. Ramadevi	Andhra Pradesh	W.S.I.
56	A. Kandaias	Andhra Pradesh	S.I., Disha P.S., Nandyal
57	Y. Sirusha	Andhra Pradesh	P.C., CyberTeam
58	M. Naga Raju	Andhra Pradesh	P.C., Disha P.S., Vijayawada
59	D.N. Subrahyan	Andhra Pradesh	Cyber Expert, Disha P.S.,
60	N. Mahesh	Andhra Pradesh	P.C. Disha P.S., AKP
61	K. Rupakala	Andhra Pradesh	W.P.C., Disha W.P.S., ASR
62	Nayan Jyoti Das	Assam	Inspector CID
63	Tapan Dass	Assam	Inspector Anti Trafficking
64	Paulus Narzary	Assam	Inspector Golapara
65	Uttam KR Deley	Assam	Inspector CID
66	Kaushik Malla Bujar Baruah	Assam	Inspector CID
67	Daisy Nath	Assam	Sub-Inspector CID.
68	Jayanta Kakoti	Assam	Pamban Chimaug
69	Ratul Haloi	Assam	Inspector PI, Dhubmi
70	Arup Jyoti Baishya	Assam	Inspector Nalbari
71	Sanjeeb KR Das	Assam	Inspector CID
72	MukutKakati	Assam	Inspector Mamgo Doi Police Station
73	Ajit Kumar Rai	Assam	Inspector Dibrugarh
74	Rimjim Mahanta	Assam	Inspector CID
75	BichitraHazong	Assam	Inspector CID
76	Jayant Kakoti	Assam	Inspector CI PanbariChimang
77	Hemanta Halol	Assam	Inspector CID
78	Arbil Hojai	Assam	Inspector CID
79	Tripti Gogoi	Assam	Inspector CID
80	Muktajur Rahman	Assam	Inspector CID
81	Ajay Barman	Assam	Inspector CID HQ
82	LongkiTerom	Assam	Inspector Biswanath DEF
83	Deep Jyoti Mazumdar	Assam	Inspector Tamulpur DEF

84	Arup Pathak	Assam	Inspector Kamrup DEF
85	Ajoy KR Saha	Assam	Inspector Bongaigaon DEF
86	Rakesh Kahita	Assam	Inspector CID
87	Nadarul Islam	Assam	Inspector CID
88	Vijay Kumar Ojha	Bihar	Inspector, Economic Offences Unit
89	Ajay Kumar	Bihar	Inspector, AHTU CID, Bihar, Patna
90	Jawad Akhtar	Bihar	Inspector EOO
91	Binod Singh	Bihar	Inspector, EOO
92	Santosh Sharma	Bihar	Inspector, SSp office, Patna, AHTU
93	Sanjeev Kumar	Bihar	Inspector of Police, EOU, Bihar, Patna
94	Kapil Deo Prasad	Bihar	Inspector, Patna
95	Vishwjit	Bihar	Inspector, Cyber police station, Gaya
96	Krishna Murari	Bihar	Inspector, Economic Offences Unit
97	Pratibha Kumari	Bihar	Sub Inspector, CID
98	Faisal Ahmed Ansari	Bihar	Inspector, Bengusarai
99	Kr. Santosh Rajak	Bihar	Inspector, Muzaffarpur
100	Amrita Rani	Bihar	Inspector, EOU
101	Sachindra Yadav	Bihar	Inspector, Jehanabad
102	Ajay Chaudhary	Bihar	Inspector SJPO
103	Ramanendra Kumar	Bihar	Inspector SJPO
104	Chaturvedi Seedhra Kumar	Bihar	Inspector EOU
105	Deo Narayan Paswan	Bihar	Inspector, EOU
106	Nagendra Paswan	Bihar	Inspector, EOU, Patna
107	Pushpalata Borkar	Goa	LPI, AHTU, Madgaon
108	Nathan De Almeida	Goa	PI, SIT (LG), Cybercrime
109	Vilas N. Patil	Goa	PSI, Cybercrime
110	Ashok Megeri	Goa	ASI, AHTU, Panaji
111	Datharam C. Gabkar	Goa	ASI, AHTU, Panaji
112	Rupali Govekar	Goa	PSI, Women PS, Panaji

113	Reema A. Naik	Goa	PSI, Women PS, Panaji
114	Suvarna Talgu	Goa	PI, GRP (E-Coy)
115	Manda M. Naik	Goa	PSI, GRP (E-Coy)
116	Adam Skaikh	Goa	ASI, GRP (E-Coy)
117	Vinayak M. Ghogali	Goa	ASI, GRP (E-Coy)
118	Lalan A. Calangutkar	Goa	LHC4567, (B-Coy)
119	Tulshi Das S. Malik	Goa	ASI, GRP (B-Coy)
120	Jitendra N. Kerkar	Goa	HC4761, (D-Coy)
121	Dilip Harmnkar	Goa	PSI, GRP (D-Coy)
122	Sanjay Gawbnoi	Goa	ASI, GRP (D-Coy)
123	Manoj P. Goltekar	Goa	ASI, GRP (E-Coy)
124	Swati Desai	Goa	LASI, Women Cell, Marga
125	Nutan U. Verenkar	Goa	DySP FRRO, WPS & AHTU
126	Sudiksha S. Naik	Goa	PI, AHTU, Margao
127	Nehanda Tavares	Goa	PSI, AHTU, Margao
128	Deepa D. Desai	Goa	PSI, AHTU
129	Pallavi P. Gawas	Goa	LASI, GRP (E-Coy)
130	Ashok S. Thanekar	Goa	PC-6391, GRP (ACoy)
131	Olga Fernandes	Goa	LHC-3805
132	BhikajiSalgaonkar	Goa	ASI, (C -Coy)
133	Prakash D. Patil	Goa	ASI, (E -Coy)
134	Yashwant P. Salgaonkar	Goa	ASI, GRP (E-Coy)
135	Nitin D. Morje	Goa	ASI, GRP (C-Coy)
136	NarsimraoTikali	Goa	PC-6916, GRP (C-Coy)
137	Amar Konadkar	Goa	PC-6098, GRP (A-Coy)
138	SripadGawas	Goa	PSI, GRP
139	Vikas Gawade	Goa	PSI, Cybercrime P.S
140	Sanit Karlekar	Goa	PSI, Cybercrime P.S.
141	Sagar Gawas	Goa	PC-7265, Cybercrime P.S.

142	Santosh Naik	Goa	PC-6213, GRP (A-Coy)
143	D.S. Vaghela	Gujarat	Dy SP, AHTU, CID
144	G.A. Patel	Gujarat	PI, AHTU, Surat City
145	Dikshit Gamit	Gujarat	PI, Cyber Cell, Surat City
146	Krupesh P. Patel	Gujarat	PI Cyber Cell, Rajkot City
147	MahendrasinhZankat	Gujarat	PI Cyber Cell, Rajkot City
148	Kalpesh S. Maniya	Gujarat	PI, AHTU, Jamnagar
149	P.M. Judal	Gujarat	PI, AHTU, Panchmahal
150	S.A. Dabhi	Gujarat	PI, AHTU, Gandhinagar
151	R.S. Damor	Gujarat	PI, Cyber Cell, Gandhinagar
152	P.U. Rana	Gujarat	PI, Cyber Cell,CID Crime, Gandhinagar
153	P.P. vaghera	Gujarat	I/C, AHTU
154	N.W. Rathwa	Gujarat	PI, AHTU, Vodadra (Rural)
155	P.A. Valvi	Gujarat	PI, AHTU, Valsad
156	A.P. Bramhbhatt	Gujarat	PI, I/C AHTU Kheda
157	Dr. B.B. Patel	Gujarat	PI, Baroda City
158	S.N. Karanjia	Gujarat	PI, Himmatnagar
159	N.N. Pargi	Gujarat	PI, Ahmedabad (Rural)
160	M.P. Pathan	Gujarat	PI, AHTU, CID
161	N.J. Jangle	Gujarat	PSI, AHTU, CID
162	K.D. Kerdiya	Gujarat	PSI, AHTU, CID
163	Arjun Oraon	Jharkhand	S.I., Jharkhand Police
164	BilkanBage	Jharkhand	S.I., Jharkhand Police
165	DulhhrmaniTudo	Jharkhand	S.I., Jharkhand Police
166	Sukhendra Yadav	Jharkhand	A.S.I., Jharkhand Police
167	Ram Pravesh Kumar	Jharkhand	INS, Bokaro
168	Bimal Kindu	Jharkhand	INS, Jamshedpur
169	Manendra Pal Roy	Jharkhand	S.I., Jharkhand Police
170	Birendra Kumar Rajabanshi	Jharkhand	Police Inspector

171	Sukant Tripathi	Jharkhand	Police Inspector
172	EduelGestenBage	Jharkhand	Police Inspector
173	Rajkapur	Jharkhand	Police Inspector
174	Kundan Kumar Verma	Jharkhand	S.I., Jharkhand Police
175	Akash Kumar Panda	Jharkhand	S.I., Jharkhand Police
176	Subodh Kumar Yadav	Jharkhand	Police Inspector, Cyber P.S., Jamtara
177	RamdeoRavidas	Jharkhand	S.I., Simdega
178	Ravi Sanjay Tapo	Jharkhand	Police Inspector, Cyber P.S., Palamu
179	Sony Xalro	Jharkhand	S.I., AHTU P.S., Sahibganj
180	Gajendra Kumar Water	Jharkhand	Inspector, CyberCrime P.S., CID Jharkhand, Ranchi
181	Kumar Sumit Yadav	Jharkhand	S.I., Jharkhand Police
182	SalanPaulkerketta	Jharkhand	S.I., Jharkhand Police
183	SubeeshmonK.S	Kerala	SI of Police
184	M.S Shibu	Kerala	SI of Police
185	Jobin George	Kerala	IP Cyber PS
186	Saranya S Devan	Kerala	SI Cyber PS , KTM
187	Kannan S P	Kerala	SI, HiTech Cell, PHQ
188	Prakash K S	Kerala	JOP,NRI Cell & Addl. Charge of Hi-Tech Cell
189	Zacharia Mathew	Kerala	Asst. Commissioner of Police, Dist. Crime Branch, Kollam City
190	Viju Kumar N	Kerala	ACP DCB
191	Sudheesh Kumar V S	Kerala	IOP Cyber PS
192	Vinod Kumar P B	Kerala	IOP Cyber PS
193	Sajeev Kumar J S	Kerala	IP Cyber, Palakkad
194	Arun M J	Kerala	IP Cyber, Malappuram
195	K J Thomas	Kerala	IP Cyber, Kochi City
196	M B Latheef	Kerala	IP CyberCrime, EKM RL
197	K Vinukumar	Kerala	IP Cyber PS, TVM RL

198	A Jayakumar	Kerala	SHO Cyber PS, Kollam City
199	Sivaprakash T S	Kerala	SHO Cyber -Crime PS, Kollam Rural
200	P Narayanan	Kerala	IP SHO Cyber PS, Kasaragod
201	Premlal S L	Kerala	IP Cyber PS, KKD RL
202	Shibu	Kerala	SI, Cyber Branch, Kollam Rural
203	Sanil Kumar	Kerala	Inspector, Cyber PS, Konni City
204	Shaju Joseph	Kerala	IP Cyber PS, Wayanad Dist
205	Mrs. Nilesh Ahirwan	Madhya Pradesh	Inspector, Cyber Cell, Jabalpur
206	Sapna Choure	Madhya Pradesh	Inspector, Cyber P.H.Q
207	Rama Masram	Madhya Pradesh	Inspector, Cyber P.H.Q
208	Anuj Samadhiya	Madhya Pradesh	S.I.
209	Indra Singh	Madhya Pradesh	Inspector
210	Renu Agul	Madhya Pradesh	T.I.
211	Ankita Khatarkar	Madhya Pradesh	ACP, Bhopal
212	Priti Tiwari	Madhya Pradesh	T.I., Indore
213	Varsha Sutavri	Madhya Pradesh	S.I. Mahila
214	Shilpa Kourav	Madhya Pradesh	Inspector, W.P.S., Bhopal
215	Mukesh Haroliya	Madhya Pradesh	Inspector, State Cyber Police, Gwalior
216	Dinesh Gupta	Madhya Pradesh	Inspector, State Cyber Police, Gwalior
217	Ram Sumer Tiwari	Madhya Pradesh	Inspector, State Cyber, Indore
218	Zaheer Khan	Madhya Pradesh	T.I., GRP Bhopal
219	Ramayan Prasad	Madhya Pradesh	Inspector, SDL
220	Shashikala Chouhan	Madhya Pradesh	S.I.
221	Lakhan Lal Vikas	Madhya Pradesh	Inspector
222	Shashikala Maskule	Madhya Pradesh	Inspector
223	Anuradha Girwal	Madhya Pradesh	Inspector
224	Dinesh Verma	Madhya Pradesh	Inspector
225	R.D. Kanwa	Madhya Pradesh	Inspector
226	Dr. Sarita Neeraj Thakur	Madhya Pradesh	Inspector (Cyber)

227	Shashi Dhurve	Madhya Pradesh	Inspector, GRP, Jabalpur
228	Girish	Madhya Pradesh	Inspector, Nimach
229	Sanjay A Pawar	Maharashtra	S.I. Sahar PS
230	Vishal Shravgi	Maharashtra	SI Cyber -Crime East Mumbai
231	Shankar Jadhav	Maharashtra	SI Cyber -Crime Thane circle
232	Manoj R Sutar	Maharashtra	PI Mumbai City
233	K.D. Aher	Maharashtra	PI Mumbai City
234	J.R Kamble	Maharashtra	PI Mumbai City
235	S.B, Khadke	Maharashtra	PI Central Cyber -Crime Unit
236	Surabhi S Pawar	Maharashtra	PI AHTU
237	Hema Chowdhry	Maharashtra	PI AHTU
238	Gajanan kadam	Maharashtra	PI Cyber Cell Navi Mumbai
239	PrithviRajGharpode	Maharashtra	PI AHTU Navi Mumbai
240	Nilam Pawar	Maharashtra	API, AHTU Navi Mumbai
241	S.S. Yadav	Maharashtra	PI Unit 7, Crime Branch Mumbai
242	Rajashri Balaji	Maharashtra	PI Unit 7, Crime Branch Mumbai
243	Nitin Potdar	Maharashtra	Spl. PI Enforcement Mumbai
244	Nilesh Khanade	Maharashtra	API Crime Branch Thane
245	Sunady Manner	Meghalaya	Inspector
246	Swedish R. Marak	Meghalaya	Inspector
247	Melissa M. Momin	Meghalaya	Inspector
248	Sandra Anny maryNongohar	Meghalaya	Dy S.P.
249	StardayKharjana	Meghalaya	Inspector
250	VijoyUdpadhya	Meghalaya	Inspector
251	Kinsheumon Tham	Meghalaya	Sub Inspector
252	Cheryl R. Kharkongor	Meghalaya	Sub Inspector
253	S. Rikseng M.Sangma	Meghalaya	Inspector
254	Fredis K. Marak	Meghalaya	Inspector

255	Handakarrhi P. Lytan	Meghalaya	Inspector
256	Kalpana Kuhari	Meghalaya	Sub Inspector
257	Neena B. Rabha	Meghalaya	Dy S.P.
258	Jessica A. Sangma	Meghalaya	Inspector
259	John Marbaniang	Meghalaya	Inspector
260	DarishaMarbaniang	Meghalaya	Constable
261	Smti Namrata Chhettri	Meghalaya	Constable
262	BrilliansiarNongsiet	Meghalaya	Constable
263	OpaiaTyngkan	Meghalaya	Inspector
264	Bopphy I. Sangma	Meghalaya	WPC Constable
265	Goalan K. Sangma	Meghalaya	Inspector
266	Animesh Mandal	Meghalaya	Inspector
267	J. Dhar	Meghalaya	Sub Inspector
268	Sambit Kumar Majhi	Odisha	DSP, Koraput
269	HaramaniBaskey	Odisha	Inspector, Sambalpur
270	Hrusikesh Behera	Odisha	Inspector, Keonjhar
271	Niranjan Sethi	Odisha	Inspector, Rourkela
272	Anand Dungdung	Odisha	DSP, Boudh
273	Manash Kumar Deo	Odisha	DSP, Balasore
274	Satya Ranjan Mallick	Odisha	ACP, CTC UPD
275	Arati Kumari Parida	Odisha	SI, CID CB, Cyber Complex
276	Banita Mharana	Odisha	Inspector,BBSR UPD
277	Kiran Mohanty	Odisha	Inspector, Nabarangpur
278	Budhadev Naik	Odisha	Inspector,GRP Rourkela
279	Satish Chandra Nayak	Odisha	Inspector, Ganjam
280	Sangram Tudu	Odisha	DSP,Jajpur
281	Sarita Mahapatra	Odisha	DSP, Kendrapara
282	Prasanta Nisika	Odisha	Inspector, Gajapati

283	SaubhangiriSethy	Odisha	ASI, CID CB, BBSR
284	Bimal Kanta Nayak	Odisha	DSP, Berhampur
285	Rashmi Rekha Mahalick	Odisha	Inspector, Mayurbhanj
286	Priya Ranjan nayak	Odisha	Inspector, Cuttack
287	ASI Satinder Singh	Punjab	I/C Social Media Cell (Patiala)
288	LR/ASI Harpal Singh	Punjab	Cyber-Crime Cell (Patiala)
289	S/CT Rajinder Singh	Punjab	CITSU (Faridkot)
290	ASI Surjit Singh	Punjab	CITSU (Hoshiarpur)
291	CT Gourav Kaushal	Punjab	Social Media Cell (SBS Nagar)
292	SI Geeta	Punjab	I/C Social Media Cell (Ferozepur Range)
293	INSP Rajinderpal Singh	Punjab	I/C Cyber-Crime Cell (Bathinda)
294	SI Bajeet Kaur	Punjab	Cyber-Crime Cell (Fatehgarh Sahib)
295	INSP Amanjot Kaur	Punjab	I/C Cyber-Crime Cell (SAS Nagar)
296	S/CT Jagdeep Singh	Punjab	I/C Social Media Cell (Tarntaran)
297	ASI Harjit Singh	Punjab	I/C Cyber-Crime Cell (Tarntaran)
298	ASI Jorawar Singh	Punjab	Computer Cell (Amritsar City)
299	CT Gourav	Punjab	Cyber-Crime Cell (SASNagar)
300	CT Harpreet Singh	Punjab	Cyber Cell (Amritsar Rural)
301	CT Rohit Verma	Punjab	Social Media Cell (Khanna)
302	CT Gurwinder Singh	Punjab	Cyber-Crime Cell
303	INSP Pushpinder Kaur	Punjab	Cyber-Crime Cell (Mansa)
304	INSP Harjit Kaur	Punjab	Cyber-Crime Cell (Sangrur)
305	SI Gurpreet Kaur	Punjab	Cyber-Crime Cell (Malerkotla)
306	SI Jyoti	Punjab	Social Media Cell (Ferozepur)
307	SI Amarjeet Kaur	Punjab	I/C Social Media Cell (Fazilka)
308	INSP Simranjeet Singh	Punjab	INT HQ

309	CT Amritpal Singh 488/PTK	Punjab	Social Media Cell (Pathankot)
310	LR/ASI Hira Singh 231/GSP	Punjab	Cyber-Crime Cell Gurdaspur
311	S/CT/ Kuldeep Singh 1368/SMS	Punjab	Cyber-Crime Cell (Muktsar Sahib)
312	ASI Pardeep Singh	Punjab	Cyber-Crime Cell (Rupnagar)
313	L/CT Manpreet Kaur	Punjab	Social Media Cell (Amritsar)
314	SI Manpreet Kaur	Punjab	CCPWC
315	SI Rupinder Kaur	Punjab	CCPWC
316	ASI Harminder Singh	Punjab	Cyber-Crime Cell (Patiala)
317	Aditya Poonia	Rajasthan	Dy SP, Rajasthan Police
318	Tej Karan	Rajasthan	CI
319	Brij Mohan Deoraj	Rajasthan	Inspector
320	Nitiraj Singh	Rajasthan	Dy SP
321	Umaid Singh	Rajasthan	Dy SP
322	Puram Mal	Rajasthan	Inspector
323	Vinod Kumar	Rajasthan	Inspector, Cyber PHQ
324	Rakesh Rajora	Rajasthan	Ad SP, Jaisalmer
325	Hari Ram Soni	Rajasthan	Dy SP, Junjhunu
326	Ramesh Tiwari	Rajasthan	Dy SP, Tonk
327	Parul Yadav	Rajasthan	SI, Cyber Thana, Ajmer
328	Shimla Devi	Rajasthan	ASI, Jaipur (Rural)
329	Preeti Beniwal	Rajasthan	CI, Mahila Thana, Sikar
330	Hari Ram Meena	Rajasthan	CI, CCPS, SOG, Jaipur
331	Ch.Gangadhar	Telangana	Inspector Cyber-Crime
332	M. Adi Murthy	Telangana	DSP CoE
333	P.Sita Reddy	Telangana	DSP CoE-CID
334	K.Venkata Lakshmi	Telangana	SP EoW
335	Padma Palle	Telangana	Inspector, CCPS

336	K.Narsimha Reddy	Telangana	Inspector. AHTU, Cyberabad
337	B.Ramreddy	Telangana	SP CMS
338	J Anyonya	Telangana	SP Admin
339	K.Shravan	Telangana	Insp. CCPS Cyber
340	A.Nandeshwar	Telangana	Inspector CCPS
341	M.Shyam Prasad Rao	Telangana	DSP, EoW
342	S.Chakrapani	Telangana	DSP CoE
343	M.Shankar	Telangana	DSP EoW
344	B.Raja Ravindra	Telangana	SI, CID
345	M.Madhu Kumar	Telangana	CI, Cyber-crime
346	Lavanya NJP	Telangana	SP, Cyber-Crime
347	P.Salomon Raj	Telangana	Inspector of Police RO, Cyberabad
348	S.Ramachnadra Reddy	Telangana	ACP, Cyberabad
349	G.Sathish Kumar	Telangana	Inspector, Cyberabad
350	N.Chandra Babu	Telangana	Inspector AHTU Rachakonda
351	P.Sangameshwar	Telangana	Sub - Inspector
352	G.Venkat Reddy	Telangana	Dy. Superintendent of Police
353	B.Saroja	Telangana	Inspector of Police
354	Ch.Suresh Babu	Telangana	Inspector of Police
355	Pranab Kanti Sahoo	West Bengal	Inspector, Diamond Harbour P.D.
356	Progati Ranjan Biswas	West Bengal	Inspector (I/C Cyber -Crime), Baruipur P.D.
357	Sudarshan Debnath	West Bengal	S.I. of Police (I/C AHTU), Baruipur P.D.
358	Tirtha Sarathi Halder	West Bengal	Inspector of Police (I/C Cyber-Crime P.S.), Diamond Harbour P.D.
359	Jyotirmoy Biswas	West Bengal	O/C Cyber-Crime P.S., CID, WB
360	Gautam Saha	West Bengal	O/C AHTU, CID, WB
361	Ajeet Kumar Jha	West Bengal	O/C Cyber-Crime, Barrackpore
362	Liton Halder	West Bengal	Inspector of Police

363	Anjana Bhowmick Ray	West Bengal	Addl O/C AHTU, CID, WB
364	Mousumi	West Bengal	S.I. of Police, O/C AHTU, Barrackpore
365	Md. Abdun Noor Chaudhury	West Bengal	S.I. of Police, Cyber-Crime PS, Bidhannagar P.C.

RESEARCH TEAM

S.No.	Name	Designation
1	Dr. Sunitha Krishnan	Principal Investigator and Advisor
2	Ms. Swasti Rana	Project Coordinator
3	Ms. Aparna Bhat	Legal Expert
4	Mr. Tabish Ahsan	Research Officer
5	Ms. Aadira Srinivasan	Assistant Legal Researcher
6	Col. Vijay Kishore Jha	Technology Expert
7	Md. Riyazuddin	Cyber Investigator



PRAJWALA

www.prajwalaindia.com