GOVERNMENT OF NATIONAL CAPITAL TERRITORY OF DELHI
(HOME–POLICE-II / ESTABLISHMENT DEPARTMENT)
5th Level, C-Wing, Delhi Secretariat, I.P. Estate, New Delhi

Order No.Home-B/65/2026-Home II/ 1950-1955 Dated : 25.08.2026

Establishment of the Delhi Cyber Crime Coordination Centre (D4C)

Sanction is hereby accorded to the establishment of the Delhi Cyber Crime Coordination Centre (D4C) as a composite nodal agency of the Delhi Police for preventing, detecting and investigating cybercrimes in the National Capital Territory of Delhi.The D4C shall function as the apex institution to support the Districts and Units of Delhi Police in addressing emerging cyber threats,and shall align its activities with those of the Indian Cyber Crime Coordination Centre (I4C), Ministry of Home Affairs, Government of India.

The objectives, jurisdiction, scope of functions, organizational structure, infrastructure, implementation framework, monitoring mechanism and miscellaneous provisions in respect of establishment and functioning of the Delhi Cyber Crime Coordination Centre (D4C) are as detailed below: -

1. Preamble

The rapid growth of digital platforms in banking, e-governance, education, commerce, and social media has resulted in concomitant proliferation of crimes such as cyber-enabled financial frauds, online radicalization, online harassment, crimes against women and children, cyber sabotage, ransomware, online incitement and public-order disruption. To effectively combat these cyber-enabled crimes, there is an urgent requirement to institutionalize/establish a Cyber Crime Coordination Centre in Government of NCT Delhi for undertaking counter-measures against these complex crimes, in alignment with the national cybercrime framework implemented under the aegis of the Indian Cyber Crime Coordination Centre (I4C).

2. Source of Policy

The establishment of D4C for National Capital Territory of Delhi is based on:

i) Information Technology Act, 2000, as amended and the Rules thereunder.

ii) Direction of Hon'ble Union Home Minister dated 26.12.2019 emphasizing standardization of cyber infrastructure in States/UTs.

iii) Recommendations of the Department - related Parliamentary Standing Committee on Home Affairs (254thReport).

iv) Order of the Hon'ble Supreme Court of India in Suo-Moto Writ Petition (Crl.) No. 03/2025 dated 01.12.2025.

3. Need for D4C in the NCT of Delhi

Delhi is the national capital territory and it houses important constitutional and administrative offices of the union and state government. Delhi is home to a large number of business establishments, corporate offices, and an upwardly mobile society, with one of the highest per capita incomes in the country.

Delhi is also a cosmopolitan city which promotes free movement, free expression and a liberal environment for creative expression. With such a diverse mix of population and activities thriving within it, the city requires a safe and secure environment, not only in the physical world, but also in the virtual space, which, over the years, has become a significant aspect of citizens' life. The D4C aims to create a state-of-the art facility that caters to all the security requirements of citizens needed for a safe and secure digital experience.

In view of the unique aspects of NCT of Delhi, and considering the evolving nature of cybercrimes, which are getting more and more complex and organized, there is an essential need for establishment of 'Delhi Cyber Crime Coordinator Centre', (D4C) to combat cybercrimes.

4. Objectives of D4C

i) To act as the nodal office for coordination with the I4C, central agencies, other States and Union Territories, regulators, financial institutions, telecom service providers, intermediaries and other stakeholders, for information-sharing, technical assistance and operational support in countering cybercrimes and enhancing cyber security.

ii) To operate facilities for generation of intelligence and surveillance over cyber threat actors in accordance with law.

iii) To operate a state-of-the-art Digital Investigation Lab to assist the Investigating Officers of all Districts and Units in deciphering digital footprints in complex cyber and conventional crimes.

iv) To operate the emergency response systems such as CFCFRMS (1930 Cyber Helpline), Fraud Mitigation Centre and other facilities, for prompt redressal of citizen grievances.

v) To plan, coordinate, organize and undertake intensive, large-scale cyber-awareness and public-outreach initiatives, in coordination with the Districts and Units.

vi) To undertake research on emerging cyber threats, new-age technologies and investigation tools; promote technological innovation in cyber policing, including through partnerships with academic institutions, start-ups, the I4C, RBI, DoT, CERT-In and MeitY; and undertake necessary implementation strategies.

vii) To strengthen the capability of Delhi Police to investigate complex cybercrimes, including online crime against women & children (OCWC) and augment its cyber-intelligence and analytics capabilities.

viii) To act as the nodal office of Delhi Police for monitoring the performance of all Districts and Units against the parameters of excellence in cyber policing, and coordinate with the Districts, Crime Branch, Special Cell, SPUWAC and other Units to facilitate the prevention, registration and investigation of cybercrimes.

ix) To plan and undertake State-wide operations against organized cybercrime syndicates and their members — such as mule-account holders, facilitators, SIM and PoS agents, hawala operatives, compromised banking-sector officials, malicious-application developers and call-centre operatives.

x) To conduct specialized training programmes, workshops and technical conferences to strengthen the capacities of police personnel and other stakeholders in the cyber ecosystem.

xi) To act as the nodal office of Delhi Police for addressing cybersecurity issues through effectiveprevention strategies, incident response & management, recovery, and detection/investigation.

xii) To undertake such other activities as may be assigned by the Commissioner of Police, Delhi, from time to time.

Establishment of the Delhi Cyber Crime Coordination Centre (D4C)

5.1 Constitution of the Delhi Cyber Crime Coordination Centre (D4C)

In pursuance of the policy directives of the Government of India for strengthening the institutional framework for combating cybercrime and in accordance with the Concept Note issued by the Ministry of Home Affairs on the establishment of State Cyber Crime Coordination Centres (S4Cs), the Government of NCT of Delhi hereby establishes the Delhi Cyber Crime Coordination Centre (D4C), as the apex cybercrime coordination and management mechanism under the administrative control of the Commissioner of Police, Delhi.

The Delhi Cyber Crime Coordination Centre (D4C) shall function as the nodal institution for coordinating cybercrime prevention, cybercrime investigation, cyber security, financial cyber fraud mitigation, capacity building, cyber awareness, research and innovation, digital forensic support, and inter-agency coordination within the NCT of Delhi.

The functions and operational activities of D4C, including intelligence generation,digital investigation and forensic support, cyber threat monitoring/surveillance,handling of digital and other data, and coordination with other agencies, shall beundertaken in accordance with law, applicable procedural safeguards, extantinstructions and the jurisdictional competence of the concernedauthorities/agencies.

5.2 Superintendence & Control

The day-to-day administrative control of the Delhi Cyber Crime Coordination Centre (D4C) shall vest in an officer of the rank of Joint Commissioner of Police, who shall be designated as the Chief Executive Officer (CEO), D4C. The CEO, D4C shall function under the direct supervision of the Special Commissioner of Police, Special Cell, and the overall supervision and control of the Commissioner of Police, Delhi. The CEO shall be assisted by Deputy Commissioners of Police heading specialized Wings in a pyramidal organizational structure. These Wings shall discharge distinct responsibilities to strengthen cybercrime prevention, investigation, enforcement and cyber security.

The Commissioner of Police, Delhi, may, from time to time, determine or revise the rank, number, designation and deployment of personnel, and the organizational structure of the D4C, in accordance with operational and administrative requirements.

5.3 Jurisdiction

The Delhi Cyber Crime Coordination Centre (D4C) shall exercise functional jurisdiction over the entire National Capital Territory of Delhi.

5.4 Operational Philosophy

The Delhi Cyber Crime Coordination Centre (D4C) shall adopt an integrated, technology-driven, and victim-centric approach to cybercrime management.

5.5Financial and Administrative Support

The expenditure for the establishment, operation, maintenance, and future expansion of the Delhi Cyber Crime Coordination Centre shall be met from:

i) budgetary allocations of the Delhi Police;

ii) assistance from the Government of India under approved schemes;

iii) grants-in-aid and centrally sponsored projects; and

iv) any other source approved by the Government.

5.6 Incentives

The CEO of the Delhi Cyber Crime Coordination Centre (D4C) may, subject to the availability of funds and separate orders, recommend the grant of suitable monetary or non-monetary incentives, special allowances, commendations, awards, career progression measures, or other recognition mechanisms for personnel serving in the Delhi Cyber Crime Coordination Centre (D4C). Such recommendation, with the approval of the Commissioner of Police, Delhi, may be considered and approved by the Government for the effective functioning of the Delhi Cyber Crime Coordination Centre (D4C).

5.7 It is further ordered that:

1. The existing Intelligence Fusion & Strategic Operations (IFSO) Unit, Dwarka, shall henceforth stand subsumed into the D4C; and its Investigation Wing, the Digital Investigation Lab, the Training & Awareness Centre, the 1930 Cyber Helpline Control Room at Haiderpur, and the Fraud Mitigation Centre (FMC) shall form an integral part of the D4C.
3. The Cyber Police Stations operational in each of the fifteen Police Districts of Delhi shall implement the cyber policies and operational directions issued by the D4C.
4. The proposal for the creation and sanction of posts of the various categories required for the D4C shall be processed separately and forwarded to the Ministry of Home Affairs for consideration and approval, in accordance with the prescribed procedure. Till the creation and regular filling of posts for the D4C, the Police Headquarters, Delhi, shall deploy the requisite number of police personnel to the D4C from the existing strength of the Delhi Police.
5. The existing tools, equipment and logistics support provisioned for the various facilities of IFSO Unit, including 1930 Helpline, Digital Investigation Lab and Fraud Mitigation Centre, shall continue to be utilized by the respective Wings of D4C. Proposals for tools, equipment and infrastructure required to implement the objectives and functions assigned to the Wings and Units of the D4C, shall be submitted by Delhi Police to the government for provisioning of budget and grant of necessary approvals and sanctions.

The organizational structure, the functions and responsibilitiesof all the Wings and the tentative requirement of tools and equipment of the Delhi Cyber Crime Coordination Centre (D4C) are appended to this Order as Annexure-A, A1 and A2.The staff strengthof all the Wings of the D4C will be separately notified as per approval of Ministry of Home Affairs.

By order of the Hon'ble Lieutenant Governor, Delhi.

25.8.26

(Santosh D. Vaidya)
Principal Secretary (Home)
Government of NCT of Delhi

Order No.Home-B/65/2026-Home II/ 1950-1955 Dated 25.08.26 Dated : 25.08.2026

SANTOSH D. VAIDYA
Principal Secretary (Home),
Government of NCT of Delhi
5th Floor, 'C' Wing, Delhi Secretariat,
New Delhi-110002

Copy to the :

1. Commissioner of Police, Delhi
2. Additional Secretary (CIS), Ministry of Home Affairs, Government of India.
3. Additional Secretary (UT), Ministry of Home Affairs, Government of India.
4. Chief Executive Officer, Indian Cyber Crime Coordination Centre (I4C), MHA.
5. Secretary to Hon'ble Lt Governor, Government of NCT of Delhi.
6. OSD to Chief Secretary, Government of NCT of Delhi.

Annexure-A

Organizational Structure, Logistics, Functions and Responsibilities

1. Organizational Structure

The Delhi Cyber Crime Coordination Centre (D4C)shall function under the overall superintendence of the Commissioner of Police, Delhi. The administrative and operational control of the D4C may be designated by the Commissioner of Police from time to time. The D4C shall be headed by a Chief Executive Officer (CEO) of the rank of Joint Commissioner of Police, who shall oversee its administration, management and functioning, assisted by Deputy Commissioners of Police heading specialized Wings in a pyramidal organizational structure. These Wings shall discharge distinct responsibilities to strengthen cybercrime prevention, investigation, enforcement and cyber security.

The Commissioner of Police, Delhi, may, from time to time, determine or revise the rank, number, designation and deployment of personnel, and the organizational structure of the D4C, in accordance with operational and administrative requirements and with approval of Competent Authority.

The D4C shall consist of the following four Wings:

i) Administrative Wing
ii) Cyber Investigation Wing
iii) Operations Wing
iv) OCWC Wing

Each Wing shall be headed by a senior supervisory officer of the rank of Deputy Commissioner of Police. The organization chart of the D4C is appended as **Annexure A1.**The organizational structure of all the Wings of the D4C and theirfunctions and responsibilities are captured as below. The staff strength and requirement of tools and equipment of all the Wings of the D4C will be separately notified as per approval of Ministry of Home Affairs.

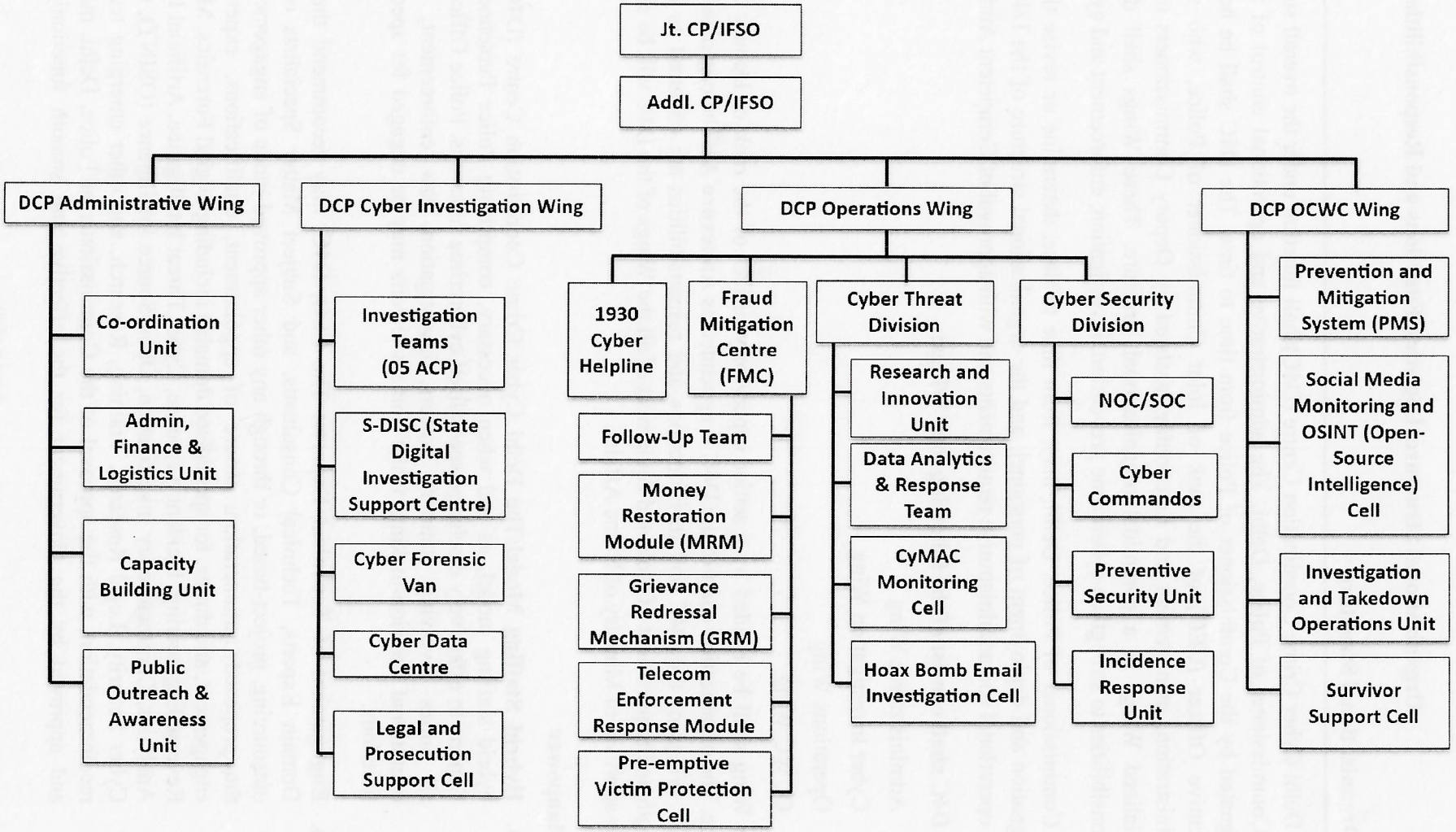
2. Manpower

a. **Hybrid Staffing Model:**The Delhi Cyber Crime Coordination Centre (D4C) shall adopt a hybrid staffing model, as and when necessary, comprising Police Personnel and Technical Experts to effectively discharge specialised cybercrime functions. Police Officers shall perform all duties involving statutory powers, investigation, law enforcement, supervision and operational decision-making, while domain experts may be engaged for specialised technical functions.

b. **Engagement of Technical Experts:** The CEO, D4C, may recommend the engagement of Domain Experts, Technical Consultants, and Subject Matter Specialists on a contractual, outsourcing, project-based, or through any other approved mode of engagement, together with the proposed remuneration, tenure of appointment, qualifications, experience, terms of engagement, and duties, for specialised domains including Digital Forensics, Malware Analysis, Reverse Engineering, Incident Response, Cyber Threat Intelligence, Artificial Intelligence, Data Analytics, Cryptocurrency Investigation, Open-Source Intelligence (OSINT), Cloud Forensics, Cyber Security, Legal Research, Training, Research, and other emerging technologies. Such recommendation, with the approval of the Commissioner of Police, Delhi, may be considered and approved by the Government for the effective and smooth functioning of the D4C.

Annexure A1

Organization Chart of the Delhi Cyber Crime Coordination Centre (D4C)



3. Tools & Equipment

The tentative requirement of tools and equipment of Delhi Cyber Crime Coordination Centre (D4C) is appended as **Annexure A2.**

4. Functions and Responsibilities of the Wings

4.1 Administrative Wing

The Administrative Wing shall have the following components: the Coordination Unit; the Admin, Finance & Logistics Unit; the Capacity Building Division; and the Public Outreach & Awareness Unit.

(a) Coordination Unit

The Coordination Unit shall act as the strategic nerve-centre and the central liaison and communication hub of the D4C. Its functions shall be:

i) Coordination of cyber operations, such as CyHawk, with other stakeholders — the Districts, the Crime Branch, the SPUWAC, other States, the I4C and other agencies.

ii) Coordination with the I4C, MHA,MeitY, CertIN and other central agencies, Ministries including Ministry of I&B, GNCT Delhi, other States and Union Territories, regulators, financial institutions, telecom service providers, intermediaries and other stakeholders, for information-sharing, technical assistance and operational support in countering cybercrimes and enhancing cyber security

iii) Coordination with police authorities outside Delhi to facilitate out-station investigations by the Delhi Police, the inter-State service of notices, the execution of warrants and the exchange of intelligence.

(b) Admin, Finance & Logistics Unit

This Unit shall manage the internal administration of the D4C, including finance, logistics and human-resource management. It shall oversee:

i) Deployment of personnel and maintenance of service records;

ii) Budget preparation, financial planning and expenditure monitoring, procurement of tools&equipment;

iii) Vehicle management, infrastructure development, and asset and inventory management.

(c) Capacity Building Unit

The Unit shall function as the nodal unit for capacity building and skill development. It shall train the personnel of Delhi Police, prosecutors and other stakeholders in cyber investigation, digital forensics and cyber law. It shall undertake the following:

i) Design and conduct basic, refresher and advanced Cybercrime Investigation Courses.

ii) Organize specialized training programmes in Digital Forensics, Malware Analysis, Open-Source Intelligence (OSINT), Cyber-Threat Intelligence and Incident Response on a regular basis.

iii) Partner with the I4C, CERT-In, academic institutions and other national and international organizations for technical training, the development of e-learning modules, simulation-based training laboratories, certification programmes, workshops, seminars, cyber-range exercises, joint threat-intelligence sharing and periodic case reviews.

iv) Conduct Internship programmes for UG & PG students of technical and professional institutions.

v) Identify, train and mentor young and senior citizens alike,who can serve as Cyber Warriors, and who may be deployed by the Public Outreach & Awareness Unit for cyber-awareness and outreach activities.

(d) Public Outreach & Awareness Unit

The Public Outreach & Awareness Unit shall promote cyber awareness and safe digital practices among citizens across the NCT of Delhi. It shall design and implement campaigns to educate the public on emerging cyber threats and cyber-enabled crimes, by leveraging social-media platforms, digital media and other communication channels to disseminate advisories, awareness content and preventive measures. In discharging these functions, the Unit shall:

i) Conduct regular outreach programmes in schools, colleges, universities, government institutions, private organizations and other public forums to promote cyber hygiene and safe digital practices; and

ii) Coordinate with Districts, Police Stations, government agencies, civil society organizations, industry partners and social-media personalities for year-round awareness campaigns and the development and dissemination of Information, Education and Communication (IEC) material;

4.2 Cyber Investigation Wing

The Cyber Investigation Wing, headed by an officer of the rank of Deputy Commissioner of Police, shall be primarily responsible for the investigation of cybercrime cases. Created by subsuming the investigative wing of the existing IFSO Unit, it shall comprise three sub-units — the Investigation Teams, the State Digital Investigation Support Centre (S-DISC), and the Legal & Prosecution Support Cell.

(a) Investigation Teams

A D4C Police Station shall be established with jurisdiction throughout the NCT of Delhi, and shall be authorized to register and investigate cybercrime cases of such nature as may be decided by the competent authority from time to time. Its functions shall be:

i) To investigate high-value, multi-victim or complex cybercrime cases.

ii) To coordinate with the National Digital Investigation Support Centre (N-DISC) and the Digital Investigation Lab for analysis of digital evidence.

(b) State Digital Investigation Support Centre (S-DISC)

The S-DISC shall provide specialized technical assistance to Investigating/Enquiry Officers of various Districts/Units of Delhi Police during different stages of their investigations/enquiries. It shall maintain advanced laboratories for mobile forensics, memory forensics, cloud forensics, network forensics,

CCTV examination and cryptocurrency investigations. It shall, within its ambit, operate Cyber Forensic Vans and a Cyber Data Centre, which shall serve as a repository of datasets pertaining to cyber investigations.

(c) Legal & Prosecution Support Cell

The Legal & Prosecution Support Cell shall function under the Cyber Investigation Wing as the specialized legal-support unit for cybercrime investigations. It shall provide legal guidance to Investigating Officers throughout the investigation, prosecution and trial stages, ensuring that investigations are conducted in accordance with the applicable provisions of law and judicial precedents. The Cell shall work in close coordination with Prosecuting Officers, Public Prosecutors and other legal authorities to improve the quality of investigation and enhance conviction rates.

4.3 Operations Wing

The Operations Wing shall function as the intelligence, analytics and predictive-policing arm of the D4C. It shall be headed by an officer of the rank of Deputy Commissioner of Police, and shall analyse crime & criminal data, digital-crime trends and behavioural patterns to detect emerging threats, hotspots and modus operandi, and to provide actionable inputs for cybercrime mitigation. It shall maintain coordination with financial institutions, telecom service providers, internet intermediaries and law-enforcement agencies for the timely exchange of information and threat indicators. The Wing shall comprise of the 1930 Cyber Helpline, the Fraud Mitigation Centre, the Cyber Threats Division and the Cyber Security Division, the last being aligned with the I4C's Cyber Security Division.

(a) 1930 Cyber Helpline

The 1930 Cyber Helpline — NCT of Delhi's Control Room of the I4C's CFCFRMS, serves as the primary citizen-contact point for reporting cyber-financial frauds, and for prompt withholding of fraudulent transactions and mitigation of financial losses. It shall also be responsible forautomatic registration of e-Zero FIRs in complaints meeting the criteria determined by Delhi Police from time to time.

(b) Fraud Mitigation Centre (FMC)

The Fraud Mitigation Centre shall function as the dedicated unit for minimizing the financial losses arising from cyber frauds, and shall follow the SOP for NCRP–CFCFRMS, lien-marking, restoration of money and grievance-redressal issued by the I4C. It shall process NCRP/CFCFRMS financial-cyber-fraud complaints in real time, secure the quickest possible response of banks in maximizing lien-marking, undertake money-trail analysis, generative pre-emptive alerts to victims of cyber frauds, and act on high-priority transactions as reflected on the D4C dashboards. It shall house representatives of the banks for this purpose.

(c) Cyber Threats Division

The Cyber Threats Division shall function as the intelligence and early-warning unit of the D4C. It shall be responsible for monitoring cyber threats, analyzing cybercrime trends, identifying emerging risks and generating actionable intelligence to support investigations, operations and informed decision-making. The Division shall comprise the Research & Innovation Unit, the Data Correlation Cell and the Financial Intelligence Cell.

i) **Research & Innovation Unit:**This Unit shall function as the knowledge and innovation hub of the D4C. It shall conduct research on emerging cyber threats, new technologies and changing criminal methodologies. It shall develop new investigative methodologies, best practices and SOPs;promote the use of AI, Machine Learning, data analytics and other advanced technologies to enhance detection, threat analysis and operational efficiency; and prepare analytical reports and recommendations for strengthening cyber policing, cyber security and cyber resilience in Delhi.

ii) **Data Analytics & Response Team:**This Team shall:

a. Provide analytical models, cyber-fraud-detection methodologies and technology-driven investigative support;

b. Maintain centralized repositories of cybercrime intelligence, fraud typologies and indicators of compromise;

c. Develop crime heat-maps, offender profiles and link-analysis reports;

d. Provide technical and analytical support to investigation teams during major investigations and State-level cyber operations.

e. Analyse financial-transaction patterns relating to cyber frauds and identify organized cybercrime syndicates.

f. Coordinate with the banks, the RBI, the NPCI, the FIU-IND, the I4C and other stakeholders; and generate strategic-intelligence inputs to support policy formulation and targeted enforcement.

iii) **CyMAC Monitoring Cell**– A dedicated CyMAC Monitoring Cell shall be operated for continuous monitoring, analysis and dissemination of cyber threat intelligence, coordination with national and State cyber security agencies, real-time tracking of emerging cyber threats/incidents, and providing analytical as well as operational support to investigation units in matters having inter-State, national or strategic cyber security implications. The Cell shall also undertake specialised investigation of cases assigned/entrusted to it.

iv) **Hoax Bomb E-mail Investigation Cell**– A separate Hoax Bomb E-mail Investigation Cell shall also be established to undertake specialised investigation of offences involving Virtual Private Networks (VPNs), anonymisation technologies, spoofed or anonymous e-mails, hoax bomb threats and other technology-enabled communications, including technical attribution, digital evidence collection, inter-agency liaison with telecom service providers, internet intermediaries and e-mail service providers, and providing expert investigative assistance to all Districts/Units of Delhi Police.

(d) Cyber Security Division

The Cyber Security Division shall be responsible for monitoring, preventing and responding to cyber-security threats affecting government systems, critical infrastructure and public digital assets. It shall also be responsible for monitoring and preventing cyber security attacks on Delhi Police's digital infrastructure. It shall conduct vulnerability assessments, cyber audits, threat-intelligence analysis, security monitoring, incident management and awareness initiatives, to strengthen cyber resilience and preparedness in Delhi Police. The following units shall operate under this Division:

i) **Network / Security Operations Centre (NOC/SOC):**The NOC/SOC shall provide continuous monitoring of networks, servers, applications, security devices and digital infrastructure of Delhi Police. It shall detect security incidents, analyse logs, generate alerts, monitor the cyber-security posture and support incident-response operations through centralized surveillance and real-time threat detection.

ii) **Cyber Commandos:**Cyber Commandos trained by the I4C, Ministry of Home Affairs, shall be deployed in the D4C to strengthen its capabilities in cybercrime prevention, investigation, threat-intelligence, incident response and digital forensics.

iii) **Preventive Security Unit:**This Unit shall focus on proactive cyber-threat prevention by conducting security checks of the Delhi police computer systems, through awareness campaigns, capacity-building programmes, the promotion of cyber hygiene, the issuance of advisories and stakeholder engagement, and shall develop preventive measures to reduce risks across computer systems in Delhi Police.

iv) **Incident Response Unit:**This Unit shall provide rapid technical and operational response to cyber incidents, security breaches, malware infections and digital emergencies. It shall conduct preliminary technical assessments, coordinate containment and recovery, support forensic acquisition, and liaise with national cyber-response agencies when required.

4.4 Online Crimes against Women & Children (OCWC) Wing

With the rapid expansion of digital media across the country, women and children have become especially vulnerable to online crimes — such as the dissemination of non-consensual intimate images (NCII), cyber-stalking, sextortion, grooming, cyber-enabled human trafficking, the circulation of Child Sexual Exploitation & Abuse Material (CSEAM) and technology-facilitated gender-based violence. Children are increasingly victimized online owing to their exposure to internet-based platforms; and AI-generated content has become a double-edged sword, being increasingly misused to produce and distribute CSEAM and sexually-explicit content. Emerging challenges in this domain include the live-streaming of the sexual abuse of children (LSAC) and the financial sextortion of children (FSEC).

The OCWC Wing shall function as the specialized Wing of the D4C for the prevention, detection and coordination of action relating to technology-enabled offences affecting women and children. It shall implement the initiatives of the I4C, and shall coordinate with the SPUWAC (Special Police Unit for Women and Children), the District Cyber Police Stations, intermediaries and other stakeholders for timely action. The Wing shall be headed by an officer of the rank of Deputy Commissioner of Police, and shall discharge its functions through its sub-units, namely the Prevention & Mitigation System (PMS), the Social Media Monitoring & OSINT Cell, the Takedown Operations Cell and the Survivor Support Cell. Its functions shall be:

i) Processing and monitoring the NCRP complaints relating to online crimes against women and children, and ensuring timely action.

ii) Generating actionable intelligence on organized online-sexual-exploitation networks, repeat offenders and cyber hotspots.

iii) Coordinating with the I4C, the SPUWAC, the District Cyber Police Stations, social-media intermediaries, internet service providers and other stakeholders for content removal, evidence preservation and enforcement.

iv) Providing investigation support in cases involving NCII, sextortion, cyber-stalking, online grooming, AI-generated sexual content, CSEAM and other cyber-enabled offences against women and children.

v) Monitoring and implementing Prevention & Mitigation System (PMS) — including the use of the Proactive Monitoring Tool (PMT), and other technology platforms developed by the I4C.

vi) Developing data-driven intelligence, analytical reports and policy recommendations using NCRP complaints, cyber intelligence and operational data.

vii) Building the capacity of Investigating Officers, and conducting awareness programmes for educational institutions, vulnerable groups and the public regarding online safety.

viii) Coordinating with counselling, legal-aid and victim-support agencies to facilitate the timely assistance and rehabilitation of victims.

Annexure –A2

Indicative Tools & Equipment Requirement
Delhi Cyber Crime Coordination Centre (D4C)

This listing sets out the indicative tools, equipment and infrastructure required to implement the objectives and functions assigned to the Wings and Units of the D4C, organised Wing-wise and Unit-wise. Quantities, exact makes/models and detailed technical specifications are to be finalised at the procurement stage based on sanctioned strength, case load, budgetary provisions and prevailing GeM/CPP Portal price discovery.

1. Digital Investigation Lab / State Digital Investigation Support Centre (S-DISC) — Cyber Investigation Wing

Core forensic laboratories providing technical assistance to Investigating/Enquiry Officers of all Districts and Units, as envisaged for the S-DISC.

S.No	Item / Equipment	Description / Purpose	Broad Specifications
1	Mobile Forensic Workstation	Extraction and analysis of data (including deleted/encrypted data) from smartphones and feature phones	High-performance workstation bundled with UFED Touch2/4PC, Cellebrite Premium, Oxygen Forensic Detective, MSAB XRY; supports Android/iOS physical, logical and file-system extraction
2	Chip-off / JTAG / ISP Forensic Rig	Data extraction at chip level from damaged, locked or bypassed devices	Chip-off adapters, JTAG/ISP boxes (e.g., Easy-JTAG Plus, RIFF Box, Medusa Pro), BGA rework/reballing station, eMMC/UFS/NAND readers
3	Computer / Disk Forensic Workstation	Imaging, indexing and analysis of hard disks, SSDs and removable media	Hardware write-blockers (Tableau/WiebeTech), forensic duplicator (e.g., Falcon-Neo/Talon), EnCase/FTK/X-Ways Forensics/Autopsy licenses, high-RAM (128GB+) multi-core workstation
4	Memory (RAM) / Live Forensics Toolkit	Volatile-memory acquisition and analysis for malware and intrusion cases	Live-acquisition tools (Magnet RAM Capture, FTK Imager, Belkasoft Live RAM Capturer), Volatility Framework, write-protected external SSD for dumps
5	Cloud Forensics Suite	Lawful acquisition and analysis of data from cloud email, storage and social-media accounts	Cellebrite Cloud / Magnet AXIOM Cloud / Oxygen Forensic Cloud Extractor on an isolated, internet-enabled workstation with secure

			logging of access
6	Network Forensics & Packet-Capture Toolkit	Capture and analysis of network traffic for intrusion, DDoS and cybercrime investigations	Wireshark, NetworkMiner, dedicated packet-capture appliance with SPAN/TAP support, high-throughput capture NIC
7	CCTV / Video Forensic Analysis Workstation	Enhancement, format conversion, frame extraction and authentication of video evidence	Amped FIVE / Amped Authenticate, proprietary multi-brand DVR/NVR player suite, GPU-accelerated video-enhancement workstation
8	Cryptocurrency Investigation Workstation	Blockchain transaction tracing, wallet clustering and exchange attribution	Chainalysis Reactor / CipherTrace Armada / Elliptic, dedicated analyst workstation with secure, logged internet access
9	Portable Field Forensic Kit	On-site acquisition of digital evidence during search/seizure	Portable write-blockers, compact forensic duplicators, labelled evidence bags, anti-static and moisture-proof containers
10	Faraday Bags / Portable Faraday Tent	Isolation of seized mobile devices from cellular/Wi-Fi signal to prevent remote wipe	RF-shielding bags in assorted sizes; a portable Faraday tent for large-scale or multi-device seizures
11	Digital Evidence Management System (DEMS)	End-to-end chain-of-custody tracking of seized digital evidence	Software platform with audit trail, hash verification, barcode/RFID tagging, integrated with case-management system
12	Secure Evidence Storage Server / Vault	Long-term, tamper-evident storage of forensic images and case data	Encrypted RAID-based NAS/SAN storage, access-controlled evidence-server room, tamper-evident lockers for physical media/exhibits

2. Cyber Forensic Vans — Mobile Deployment Units (S-DISC)

For on-site acquisition support at crime scenes/incident locations across the fifteen Police Districts.

S.No	Item / Equipment	Description / Purpose	Broad Specifications
1	Mobile Forensic Van	On-site digital-evidence acquisition and preliminary triage at scene of crime	Customised vehicle fitted with a compact mobile-forensic workstation, mobile/computer forensic acquisition kits, satellite/4G-5G connectivity, and secure onboard evidence storage

2	Vehicle-mounted Power Backup	Uninterrupted power supply for onboard forensic equipment while in the field	Inverter with battery bank, sized to sustain workstation and lighting load for extended on-site operations

3. Cyber Data Centre & Core IT/Networking Infrastructure

Backbone infrastructure supporting all Wings of the D4C on a 24×7 basis.

S.No	Item / Equipment	Description / Purpose	Broad Specifications
1	Server Racks & Compute Servers	Hosting of D4C applications, dashboards, case-management systems and databases	Rack-mounted enterprise servers with virtualization (VMware/Hyper-V), redundant power supplies, hot-swappable drives
2	Enterprise Storage (SAN/NAS)	Centralised storage for case data, forensic images, CCTV footage and call recordings	High-capacity RAID storage with tiered/archival storage classes and encryption-at-rest
3	Core Network Switches & Routers	Backbone LAN/WAN connectivity across all D4C Wings and Units	Layer-3 managed switches, redundant routers, VLAN segmentation for lab/office/public-facing zones
4	Next-Generation Firewall (NGFW)	Perimeter security and traffic inspection for the D4C network	NGFW with integrated IPS/IDS, application-layer filtering and secure VPN gateway for remote/District access
5	Data Backup & Disaster-Recovery System	Continuity and recoverability of case, forensic and dashboard data	Automated backup software, offsite/DR replication, tape or air-gapped/cloud backup with tested restore procedures
6	Biometric Access Control System	Restricted, logged physical access to labs, server room and evidence vault	Biometric/RFID access readers at all sensitive-zone entry points, integrated visitor-log and intrusion-alarm system
7	Precision Air-Conditioning & Fire Suppression	Environmental control for the server room and forensic hardware	Precision cooling units with N+1 redundancy, clean-agent (e.g., FM-200/inert-gas) fire suppression, temperature/humidity monitoring
8	Uninterruptible Power Supply (UPS) & DG Backup	Uninterrupted power for round-the-clock operations	Online double-conversion UPS sized to critical load, diesel generator with automatic changeover

4. 1930 Cyber Helpline (Control Room, Operations Wing)

Augmentation of the existing Haiderpur facility to support scaled call-taker strength.

S.No	Item / Equipment	Description / Purpose	Broad Specifications
1	IP-based Contact-Centre Platform / EPABX	Call routing, IVR and recording for the 1930 helpline	Contact-centre software with IVR, Automatic Call Distribution (ACD), 100% call recording and CTI integration with the case-registration system
2	Call-taker Workstations	Ergonomic desks for scalable call-taker strength across shifts	Noise-cancelling headsets, dual-monitor setup, terminal integrated with NCRP/CFCFRMS and e-Zero FIR registration modules
3	Real-time Supervisory Dashboard / Video Wall	Monitoring of call volumes, SLA adherence and case disposal in real time	Large-format video-wall display fed by the dashboard/analytics platform
4	NCRP / CFCFRMS Integration Terminals	Direct, authenticated access to the national complaint-registration and lien-marking portal	Secure terminals with role-based access to NCRP, CFCFRMS and I4C systems

5. Fraud Mitigation Centre (FMC)— Operations Wing

For real-time processing of financial-fraud complaints and coordination with bank representatives housed at the FMC.

S.No	Item / Equipment	Description / Purpose	Broad Specifications
1	Bank-Liaison Workstations	Dedicated desks for bank representatives posted at the FMC	Networked workstation with access to respective bank lien/hold portals and a dedicated recorded telephone line
2	Transaction / Lien-Monitoring Dashboard	Real-time tracking of high-priority transactions and lien-marking percentage	Custom dashboard integrated with the CFCFRMS data feed, configurable alerts for high-value/time-critical transactions
3	Secure Hotline for Bank Coordination	Rapid, recorded communication with bank nodal officers for lien-marking	Dedicated hotline extensions with call-recording and priority routing

6. Cyber Threats Division — Research & Innovation Unit / DART / Financial Intelligence Cell

Analytics, OSINT and threat-intelligence capability supporting investigations and strategic decision-making.

S.No	Item / Equipment	Description / Purpose	Broad Specifications
1	OSINT Investigation Suite	Open-source intelligence gathering on threat actors, syndicates and mule networks	Licensed OSINT/link-analysis tools such as Maltego and SpiderFoot, plus subscription access to social-media and public-record aggregators
2	Threat Intelligence Platform (TIP)	Aggregation and correlation of Indicators of Compromise (IOCs) across cases	Commercial or MISP-based TIP with curated threat-feed subscriptions
3	Data Analytics & Visualisation Workstations (DART)	Crime heat-maps, link-analysis, offender profiling and trend analytics	High-RAM analyst workstations with BI/link-analysis software (e.g., i2 Analyst's Notebook, Power BI class tools)
4	Financial Transaction Analytics Software	Detection of organised-fraud patterns from financial-transaction data	Specialised fraud-analytics/AML-pattern-detection software with secure data-connectivity for coordination with banks, RBI, NPCI and FIU-IND

7. Cyber Security Division — Network/Security Operations Centre (NOC/SOC)

For continuous monitoring, incident response and vulnerability management of Delhi Police's digital infrastructure.

S.No	Item / Equipment	Description / Purpose	Broad Specifications
1	SIEM Platform	Centralised log correlation, alerting and audit trail across Delhi Police's digital infrastructure	Enterprise SIEM (e.g., Splunk/QRadar/ELK-based) with integration of network, server and application log sources
2	SOC Analyst Workstations & Situational-Awareness Video Wall	Round-the-clock monitoring of network and security posture	Multi-monitor analyst stations and a large-format video wall displaying live security dashboards
3	Vulnerability Assessment & Penetration Testing (VAPT) Toolkit	Periodic security assessment of Delhi Police systems and applications	Scanning tools such as Nessus/Qualys, Burp Suite, and a dedicated penetration-testing workstation
4	Endpoint Detection & Response (EDR) Suite	Detection and response to endpoint-level threats across the Delhi Police network	Enterprise EDR licenses for deployed endpoints with a central management console

5	Incident Response (IR) Field Kit	Rapid, on-site technical response to security breaches and malware incidents	Portable IR kit with live-response acquisition media, network taps, and write-blockers for first responders

8. Cyber Commandos (I4C-trained) — Deployment Equipment

Individual equipment for Cyber Commandos deployed to strengthen prevention, investigation and incident-response capability.

S.No	Item / Equipment	Description / Purpose	Broad Specifications
1	Cyber Commando Workstation	Function-specific workstation for deployed Cyber Commandos	High-specification workstation configured with the forensic, OSINT or threat-intelligence toolset relevant to the Commando's assigned function

9. Online Crimes against Women & Children (OCWC) Wing

Equipment for the Prevention & Mitigation System (PMS), Social Media Monitoring/OSINT, Takedown Operations and Survivor Support sub-units.

S.No	Item / Equipment	Description / Purpose	Broad Specifications
1	Proactive Monitoring Tool (PMT) Terminal	Access to the I4C's Prevention & Mitigation System for detection of CSEAM/NCII content	Secure, authenticated terminal integrated with the I4C PMS/PMT platform, restricted-access workstation
2	Social Media Monitoring & OSINT Workstation	Monitoring of social-media platforms for OCWC-related content, repeat offenders and hotspots	Licensed social-listening/OSINT tools with screen-capture and evidence-preservation software
3	Content Takedown Coordination System	Tracking and coordination of takedown requests with intermediaries within SLA	Case/workflow-management software with an intermediary-contact database and SLA-tracking dashboard
4	Survivor Support / Child-Friendly Interview Room	Recording of statements of women and child survivors in a safe, non-institutional setting	Soundproofed room with one-way observation provision, video/audio recording system, and comfortable furnishing appropriate for vulnerable witnesses
5	Secure Evidence Preservation Terminal (NCII/CSEAM)	Preservation of highly sensitive evidentiary content under strict access control	Isolated, access-controlled workstation with encrypted storage and comprehensive audit logging

10. Capacity Building Unit — Training & Awareness Centre

Infrastructure for basic, refresher and advanced courses, workshops, and cyber-range exercises under the Capacity Building Unit.

S.No	Item / Equipment	Description / Purpose	Broad Specifications
1	Cyber Range / Simulation Lab	Hands-on simulated attack-and-defence training for personnel	Virtualised cyber-range platform on an isolated training network with scenario-injection capability
2	Classroom AV & E-Learning Infrastructure	Delivery of classroom training, webinars and certification programmes	Projector/interactive smart-board, video-conferencing endpoint, and a Learning Management System (LMS) server for e-learning modules
3	Forensic Training Lab	Practical hands-on training for trainees on core forensic tools	Training-licensed instances of key forensic software on a dedicated set of lab workstations, mirroring the S-DISC toolset at reduced scale

11. General / Common Facility Infrastructure

Facility-wide items applicable across the D4C premises.

S.No	Item / Equipment	Description / Purpose	Broad Specifications
1	Structured Cabling & Wi-Fi Access Points	Reliable networked connectivity throughout the facility	Cat6/Cat6A structured cabling with enterprise-grade Wi-Fi access points
2	Facility CCTV Surveillance	Physical-security monitoring of the D4C premises	IP CCTV cameras with NVR, integrated with the biometric access-control system
3	Video-Conferencing System (Command/Conference Room)	Coordination meetings with I4C, other States/UTs and stakeholders	Enterprise video-conferencing endpoint with large display in a dedicated conference room