



TAMIL NADU GOVERNMENT GAZETTE PUBLISHED BY AUTHORITY

No. 32A]

CHENNAI, WEDNESDAY, AUGUST 12, 2026
Aadi 27, Parabhava, Thiruvalluvar Aandu-2057

Part II—Section 2 (Supplement) NOTIFICATIONS BY GOVERNMENT

HOME DEPARTMENT

(POLICE-XII)

Designating the existing Cyber Crime Wing Headquarters, Tamil Nadu as the Tamil Nadu State Cyber Crime Coordination Centre (TN-S4C) for the State, in accordance with the Concept Note issued by the Ministry of Home Affairs.

[G.O. Ms. No.242, Home (Police-XII), 28th July 2026,
ஆடி 12, பராபவ, திருவள்ளுவர் ஆண்டு-2057.]

No.II(2)/HO/631/2026.—

Whereas, the Hon'ble Supreme Court of India, in its Order dated 01.12.2025 in Suo Moto Writ Petition (Crl.) No.03 of 2025 has directed the Union and States/Union Territories to establish and operationalise the mechanism for effective coordination between Union and States/Union Territories in matters concerning "Digital Arrest";

And Whereas, the Ministry of Home Affairs, Government of India, vide Letter No.22003/05/2026-CC dated 09.06.2026, has advised all States and Union Territories to establish and operationalise State Cyber Crime Coordination Centre (S4Cs) as State-level nodal agencies for prevention, detection, investigation, prosecution support and coordinated response to cybercrime and has circulated a detailed Guidelines and Framework for the States and Union Territories for establishment of said centres;

And Whereas, the State Cyber Crime Investigation Centre located at the Cyber Crime Wing headquarters, Chennai has already been declared as a police station with jurisdiction over the whole of the State of Tamil Nadu by invoking the powers conferred under clause (s) of section 2 of the Code of Criminal Procedure, 1973 (Central Act 2 of 1974) vide Notification No.2/Ho/187/2022 published in the *Tamil Nadu Government Gazette* dated 30.03.2022;

AND WHEREAS, the Director General of Police/Head of Police Force, Tamil Nadu in his letter dated 14.07.2026 and 21.07.2026 requested the Government to notify the existing specialized division as the Tamil Nadu State Cyber Crime Coordination Centre (TN-S4C) at Chennai, thereby achieving complete alignment with the National Frameworks;

Now, therefore, the Government of Tamil Nadu hereby directs that the Cyber Crime Wing, in addition to its existing functions as a Police Station, shall serve as the Tamil Nadu State Cyber Crime Coordination Centre (TN-S4C) at Chennai; as a dedicated/specialized police Unit for the coordination, prevention, detection, investigation, and prosecution of cyber crimes across the State. The Centre shall function as the State nodal agency for cyber crime coordination and shall facilitate inter-agency cooperation, intelligence sharing, capacity building, cyber forensic support,

and other measures necessary for the effective enforcement of laws relating to cyber offences. The Tamil Nadu State Cyber Crime Coordination Centre (TN-S4C) shall comprise of the CCW State Headquarters at Chennai including the state Cyber Crime Police Station at the Headquarters, viz. State Cyber Crime Investigation Centre (SCCIC). Further the Cyber Crime Police Stations in Districts/City Police Commissionerates and Special Units notified by the Government, function under the administrative control of respective Unit Officers in Districts, Commissionerates and Special Units, viz. Economic Offences Wing (EOW), Crime Against Women and Children (CWC) and Narcotics Intelligence Bureau CID & Intellectual Property Rights Enforcement Cell (NIBCID & IPREC).

Prelude

There has been an upsurge in the usage of Information Communication Technology by individuals, organizations and Government bodies across the world due to rapid decline in the cost of computer systems, internet connectivity and ease of communication. Dependency of individuals on digital gadgets such as Mobile Phone, Computers, Laptops, Tablet and Computers are increasing day by day in this "Digital Era". Exponential growth in cyber space including the financial and commerce transaction and cyber users has naturally been accompanied by huge increase in cyber crimes including those involving financial frauds, cyber espionage or disruption of critical information infrastructures.

Incumbent Organizational Structure:

To address the growing challenges posed by cyber crime, the Government of Tamil Nadu had undertaken several initiatives to strengthen the institutional framework for investigation of cyber crimes in the State. As part of these measures, dedicated Cyber Crime Police Stations were established in every District and Commissionerate with the requisite administrative, financial and technical infrastructure to facilitate prompt registration and investigation of cyber crime cases in the Government order first read above.

Creation of awareness is felt as the need of the hour as in case of cyber crime, 'Prevention is better than cure'. Hence the Government of Tamil Nadu has conceptualized 'Cyber Arangam' as a collaborative public-private initiative to proactively address the rapidly evolving cyber threat landscape in the Government Order second read above. The initiative aims to leverage the expertise of academia, industry, research institutions, financial institutions and law enforcement agencies to strengthen cyber crime prevention, cyber intelligence, cyber forensics, incident response, research, training and public awareness, thereby enhancing the State's overall cyber security and cyber crime investigation capabilities.

Considering, the technicalities involved and the need for professional guidance and to facilitate State / National / Global level liaison work and to guide and supervise the Cyber Crime Police Stations formed in every district and every city, the post of the Additional Director General of Police was created in the Government Order third read above.

In view of the increasing sophistication of cyber offences, including cases involving multiple jurisdictions, organized cyber crime syndicates, ransomware, cryptocurrency, social media abuse and offences requiring specialized technical expertise, the Government of Tamil Nadu further established the State Cyber Crime Investigation Centre (SCCIC) at the Cyber Crime Wing Headquarters, Chennai, vide the Government Order fourth read above with dedicated manpower, infrastructure and specialized investigation units to undertake complex cyber crime investigations and provide centralized technical support to the field formations and it has been notified as Police Station with its jurisdiction as whole State of Tamil Nadu in the Government Order fifth read above.

Pursuant to the trifurcation of the Greater Chennai Police Commissionerate in the Government Order sixth read above, the Tambaram and Avadi Police Commissionerates were established, and a Cyber Crime Police Station was created in each of the newly formed Commissionerates.

Four Cyber Crime Police Stations for the North, South, East and West Zones under the Greater Chennai Police were established in the Government Order seventh read above thereby strengthening specialised cyber crime investigation and enhancing citizen access to cyber crime policing services in Greater Chennai Police limits.

Consequent to the formation of Mayiladuthurai District, a dedicated Cyber Crime Police Station was established for the district in the Government Order eighth read above thereby strengthening the cyber crime investigation framework and enhancing access to specialised cyber policing services.

In view of the increasing number of Cyber Crimes and difficulties in freezing and recovering proceeds of crime due to delay in registration of cases, the Hon'ble High Court of Madras in the judgment dated 29.01.2020 in CrI.O.P No.34166 of 2019 directed to create one Cyber Cell in each Police Station. Accordingly, Cyber Cell was formed with Cyber Supporting Officers in the rank of SSI, assisted by one Grade I Police Constable and station receptionist in each Police Station vide Chief Office circular in the reference ninth cited.

TN-S4C

The State Cyber Crime Coordination Centre (S4C) is envisaged as state-level counterpart of Indian Cyber Crime Coordination Centre (I4C), with a broader and more intensive mandate encompassing criminal investigation, cybercrime prevention, and cybersecurity response capabilities. The constitution of S4C is consistently emphasised by all three pillars of the State, namely the Executive, the Legislature, and the Judiciary.

In view of this, the Government of Tamil Nadu hereby resolves that the Cyber Crime Wing shall serve as **Tamil Nadu State Cyber Crime Coordination Centre (TN-S4C)**. The details of the Centre are as follows:

1. Organization, Jurisdiction and Role:

- (i) The institution shall be known as “TN-S4C”.
- (ii) It shall be located at Cyber Crime Wing Administrative Building, PTC Complex, Ashok Nagar, Chennai – 600083.
- (iii) It shall function as the State-level institution responsible for coordinating and addressing emerging cyber threats in Tamil Nadu.
- (iv) It shall function under-
 - (a) Overall supervision of the Director General of Police/ Head of Police , Tamil Nadu State.
 - (b) The immediate administrative control shall vest with the Director General of Police/ Additional Director General of Police, Cyber Crime Wing.
- (v) The review of Cyber Crime Police Stations in Units is undertaken by Zonal Superintendents of Police of Cyber Crime Wing to understand the patterns of cyber crimes in overall state and also for statistical purposes.
- (vi) TN-S4C will serve as the State Nodal agency of Indian Cyber Crime Coordination Centre (I4C).
- (vii) The immediate administrative controlling authority of the TN-S4C shall function as the State Nodal Officer for coordination with the I4C.

2. Scope and Operational Role:

TN-S4C's Scope and operational role is as follows:

- (i) To function as the State level operation command and coordination centre.
- (ii) To facilitate near real-time response, financial fraud intervention, cyber threat monitoring, cyber patrolling, etc. proactively.
- (iii) To serve as State's 24x7 operational hub for reporting the cyber incidents.
- (iv) To act as inter-agency coordination centre.
- (v) To provide operational support to District Cyber Crime Police Stations (CCPS) and other law enforcement agencies.
- (vi) To undertake real policing problems in cyber world and to provide innovative solutions to the problems.
- (vii) To coordinate with the Social Media Intermediaries taking the role of State Nodal Agency.
- (viii) To investigate cyber crime cases that require inter-state, international or multi-jurisdictional coordination. The Centre investigates cases involving organised cybercrime syndicates, ransomware attacks, cryptocurrency-related offences, large-scale financial frauds, social media offences affecting constitutional authorities, activities prejudicial to the sovereignty and integrity of India, dissemination of fake news affecting public order, and other technologically sophisticated cyber offences requiring specialised expertise.
- (ix) To provide technical guidance and investigative support to law enforcement agencies across the State
- (x) To promote cyber security awareness and foster a culture of safe and responsible digital behaviour among all sections of society.
- (xi) To build a cyber-aware and cyber-resilient community through collaboration with academia, industry and Government.
- (xii) Utilise the State-of-the-art Cyber Forensic Laboratory/ or Mobile Forensic laboratories with the advanced cyber forensic tools to cater to the needs of cyber investigation.
- (xiii) To develop, maintain and deploy advanced digital forensic tools and technologies for scientific examination, analysis and preservation of digital evidence.
- (xiv) To provide cutting-edge technical support, forensic innovation and expert assistance for cyber crime investigations across the State.
- (xv) To conduct periodical Hackathons and Internships to encourage the students to use their logical and coding skills in solving the policing problems.

(xvi) To develop annual training calendar/programme schedule for the Centre and its Police Personnel.

(xvii) To impart technical and upgraded cyber skills by conducting capacity building programmes through various institutes and cyber experts.

3. Responsibilities and Supervisory Authority:

The TN-S4C shall function as the apex supervisory authority for all Cyber Crime Police Stations in the State and shall:

- (i) exercise overall supervisory oversight over the Cyber Crime Police Stations functioning across the State under the administrative control of Unit Officers.
- (ii) issue policies, Standard Operating Procedures (SOPs), operational guidelines, advisories and circulars for uniform implementation of cyber crime prevention, investigation and cyber security measures.
- (iii) monitor registration, investigation, detection, disposal and prosecution of cyber crime cases and review the performance of field units through periodic reviews and to provide technical guidance and operational support to field Investigation Officers.
- (iv) prescribe standardized formats for submission of daily, weekly, fortnightly, monthly, quarterly and special reports by CCPS and monitor compliance.
- (v) maintain a centralized State-level cyber crime dashboard for monitoring complaints, financial fraud response, investigations, arrests, recoveries, seizures and conviction statistics.
- (vi) coordinate with Unit Officers in the State Police Department, Government Departments, Banks, Financial Institutions, Telecom Service Providers, Internet Service Providers, Intermediaries, CERT-In, I4C, RBI and other central agencies.
- (vii) coordinate State-wide cyber operations, special drives, enforcement initiatives and cyber crime prevention campaigns.
- (viii) monitor the implementation of cyber security awareness programmes, capacity building initiatives and public outreach activities undertaken through Cyber Arangam and Cyber Crime Police Stations.
- (ix) develop and maintain operational databases, cyber threat intelligence repositories and analytical systems to support intelligence-led policing.
- (x) evaluate emerging cyber threats and recommend policy interventions, technological upgrades and capacity enhancement measures to the Government.
- (xi) collect, compile, analyse and disseminate cyber crime statistics, trend analysis and best practices for improving cyber policing across the State.
- (xii) perform such other functions as may be entrusted by the Government or the Director General of Police/Head of Police Force from time to time.
- (xiii) As per Reference 13th cited, the ACRs of the Police Personnel of and above the rank of Inspectors of Police shall be written by the Officers of Cyber Crime Wing following the usual hierarchy.
- (xiv) As per Reference 13th cited, Prior approval/permission of the Director General of Police/ Additional Director General of Police, Cyber Crime Wing should be obtained in transfer, posting, promotion and all other departmental proceedings from the rank of Inspector of Police serving in Cyber Crime Police Stations.

4. Organizational Structure and Supervisory Authority:-

The Organizational structure of the TN-S4C shall be as under:

Sl. No.	Verticals	Functions and Objectives of Unit
1.	State Cyber Command Centre (SCCC):	- Headed by the Superintendent of Police, Cyber Crime Division – I. - Monitors and supervises Cyber Crime Police Stations in Chennai City, Tambaram City, Avadi and Special Units. - Operates a 24x7 control room for the 1930 Cyber Crime Helpline. - Oversee registration and processing of e-Zero FIRs relating to cyber crime, received electronically. - Facilitates Subscriber Identity Module(SIM) and International Mobile Equipment Identity(IMEI) blocking for mobile numbers suspected to be involved in cyber crime. - Coordinates content blocking based on requests received from districts, cities and Special units. - Conducts proactive cyber patrolling to detect and mitigate cyber threats. - Focuses on Open Source Intelligence (OSINT), Social Media Intelligence, Dark Web Surveillance, Online illegal activities and emerging cyber threats. - Undertakes pre-emptive identification and rescue of potential victims through cyber intelligence. - Acts as State Nodal Officer for Cyber Slavery. - Functions as the State Nodal Agency for the Central Equipment Identity Register (CEIR) portal to facilitate tracing of lost mobile phones. - Monitors inter-state arrests through the Samanvay portal. - Oversees the deployment of the State representative to the Cyber Fraud Mitigation Centre (CFMC). - Acts as Nodal Authority for e-Zero FIR cases. - Studies MOs and analyses the trend.
2.	State Cyber Crime Investigation Centre (SCCIC):	- Headed by the Superintendent of Police, Cyber Crime Division–II. - Monitors and supervises Cyber Crime Police Stations in North Zone and West Zone. - Investigates cybercrime cases where the jurisdiction of the complainant and the suspect cannot be clearly determined. - Handles cases involving victims spread across multiple jurisdictions. - Investigates incidents of social media abuse targeting constitutional authorities and other key public functionaries. - Deals with offences that threaten the sovereignty, integrity, and security of the State or the Nation. - Investigates cyber offences involving anti-national activities and the dissemination of false or inflammatory information on sensitive issues. - Handles cases involving the publication or circulation of content, including images and videos, that may affect the sovereignty and integrity of India or disturb public order.

		• Investigates organized cyber crime requiring international cooperation and cross-border coordination. • Handles complex interstate cybercrime cases, including specialized offences such as ransomware, cryptocurrency-enabled crimes and other technically sophisticated investigations that require expertise beyond the police station level. • Will take up investigation of Cyber Crime cases on the instructions of the Director General of Police/Head of Police Force in consultation with the Director General of Police/ Additional Director General of Police, Cyber Crime Wing. • Will act as e-Police station for the registration of e-Zero FIR for the cases where the money lost is above Rs.1,00,000/- • Leverages cyber experts empanelled under G.O.(D) No. 113, Home (Pol.XII) Department, dated 29.01.2025, through the Cyber Crime Wing Headquarters (CCW Hqrs.) to support specialized investigations.
3.	Cyber Arangam	• Headed by the Superintendent of Police, Cyber Arangam. • The Unit is dedicated to: (i) Promoting public awareness on various cyber crime modus operandi and the 1930 Cyber Crime Helpline. (ii) Organizing short-, medium-, and long-term training and capacity-building programmes for personnel serving in Cyber Crime Police Stations. (iii) Conducting internship programmes for students to enhance cyber crime awareness and practical exposure. (iv) Organizing hackathons to encourage innovation and strengthen cyber security capabilities. (v) Undertaking outreach initiatives to promote cyber safety and digital literacy among the public. (vi) Developing Information, Education and Communication (IEC) materials for cyber awareness and education. (vii) Conducting refresher training programmes to continuously enhance the knowledge and skills of police personnel. (viii) Preparation of annual training calendar besides annual outreach programme.
4.	Advanced Cyber Forensic Unit	• Headed by the Superintendent of Police, Cyber Crime Division-I. • To manage and maintain the existing state-of-the-art Cyber Forensic Laboratory, ensuring its effective utilization for advanced digital investigations, forensic analysis, and technical support to cybercrime investigations. • To identify, evaluate, and facilitate the deployment of advanced cyber forensic tools and technologies that enhance investigative capabilities, improve efficiency, and support evidence-based cyber crime investigations.

		• To assess, validate, and operationalize the outcomes, solutions, and prototypes developed through hackathons and internship programmes after conducting necessary vulnerability assessments, security audits, and compliance checks. • To explore, evaluate, and promote the adoption of open-source tools and technologies for strengthening cyber investigations, digital forensics, threat analysis and capacity-building initiatives.
5.	Admin Division	• Headed by the Superintendent of Police, Cyber Crime Division–III. • Monitors and supervises Cyber Crime Police Stations in South Zone and Central Zone. • The Unit is responsible for: (i) Ensuring adequate deployment of manpower to meet the operational requirements of the Cyber Crime Wing. (ii) Managing transfer, posting, and promotion-related matters of police personnel and supporting staff. (iii) Facilitating tenure exemptions for trained police personnel serving in the Cyber Crime Wing to retain specialized expertise and operational continuity. (iv) Coordinating logistical requirements and administrative support for effective functioning of the Units. (v) Processing and giving effect to incentive mechanisms, including special allowances, rewards, recognition, and other non-monetary benefits, in line with practices followed by specialized units handling counter-terrorism and anti-narcotics operations (as envisaged by I4C). (vi) Initiating and managing procurement processes, including floating tenders for required hardware, software, and technological resources. (vii) Collecting, consolidating, and analyzing data received from all Cyber Crime Police Stations to support monitoring, planning, and decision-making. (viii) Ensuring the availability of adequate infrastructure, workspace, and operational facilities for the effective functioning of the Cyber Crime Wing units. (ix) Planning and facilitating the establishment of State-level Cyber Fraud Mitigation Centre as multi-stakeholder proactive response centre for prevention, detection, and mitigation of cyber fraud.

6	Cyber Security Division	• SP/CCD-I shall serve as the nodal authority for ensuring preventive cyber security and protection of the IT assets, digital infrastructure, and critical information systems of the Police Department, functioning in the capacity of the Chief Information Security Officer (CISO). • The Division shall be responsible for formulating and implementing cybersecurity policies, conducting risk assessments, strengthening security controls, monitoring cyber threats and ensuring continuous protection of departmental digital resources. • The Division shall act as the primary incident response unit for major cyber security incidents affecting Police Department systems and digital infrastructure, coordinating detection, containment, mitigation, recovery, and post-incident analysis. • The Division shall leverage the expertise and capabilities of trained Cyber Commandos to provide rapid technical response, digital threat analysis, and specialized support during significant cyber security incidents. • The Division shall also coordinate with relevant stakeholders, cyber security agencies and technical experts to enhance the overall cyber resilience and preparedness of the Police Department.
---	--------------------------------	--

5. Institutional Experts/ Multi-Disciplinary Expertise and Outsourcing:

- (i) The Government have accorded sanction for a sum of Rs.1,00,00,000/- vide Government Order tenth read above, as recurring expenditure for Hiring of the Institutional Experts for Cyber Crime Wing. Accordingly, Cyber Crime Wing has empanelled six experts who are specialized in Log analysis, VAPT, Dark Web investigation, Threat Intelligence Analysis, Security breach investigation, Digital and Mobile Forensics, Management & Strategy and Malware analysis.
- (ii) The team for the tool selection of the Advanced Cyber Forensic Unit shall be sourced through deputation from various wings of the Police Department, as well as from organizations such as TNeGA, IIT Madras, NFSU, and other specialized departments identified by the Head of the Cyber Crime Wing. This team shall leverage multi-disciplinary expertise to evaluate, identify, and finalize advanced cyber forensic tools and technologies aligned with emerging cyber crime trends and operational requirements.
- (iii) The Government have accorded a sanction of Rs. 8.88 crores *vide* Government Order eleventh read above, towards the expansion of National Cyber Crime Helpline 1930 Call Centre with 15 seaters (outsourced) for 3 years.
- (iv) The Government have accorded sanction of a sum of Rs.6,00,000/- for creating a post of Legal Advisor to Cyber Crime Wing on contract basis at Rs.50,000/- per month.

6. Periodic Review

The performance of each vertical of TN-S4C shall be reviewed in the following manner:-

(i) Monthly Review:

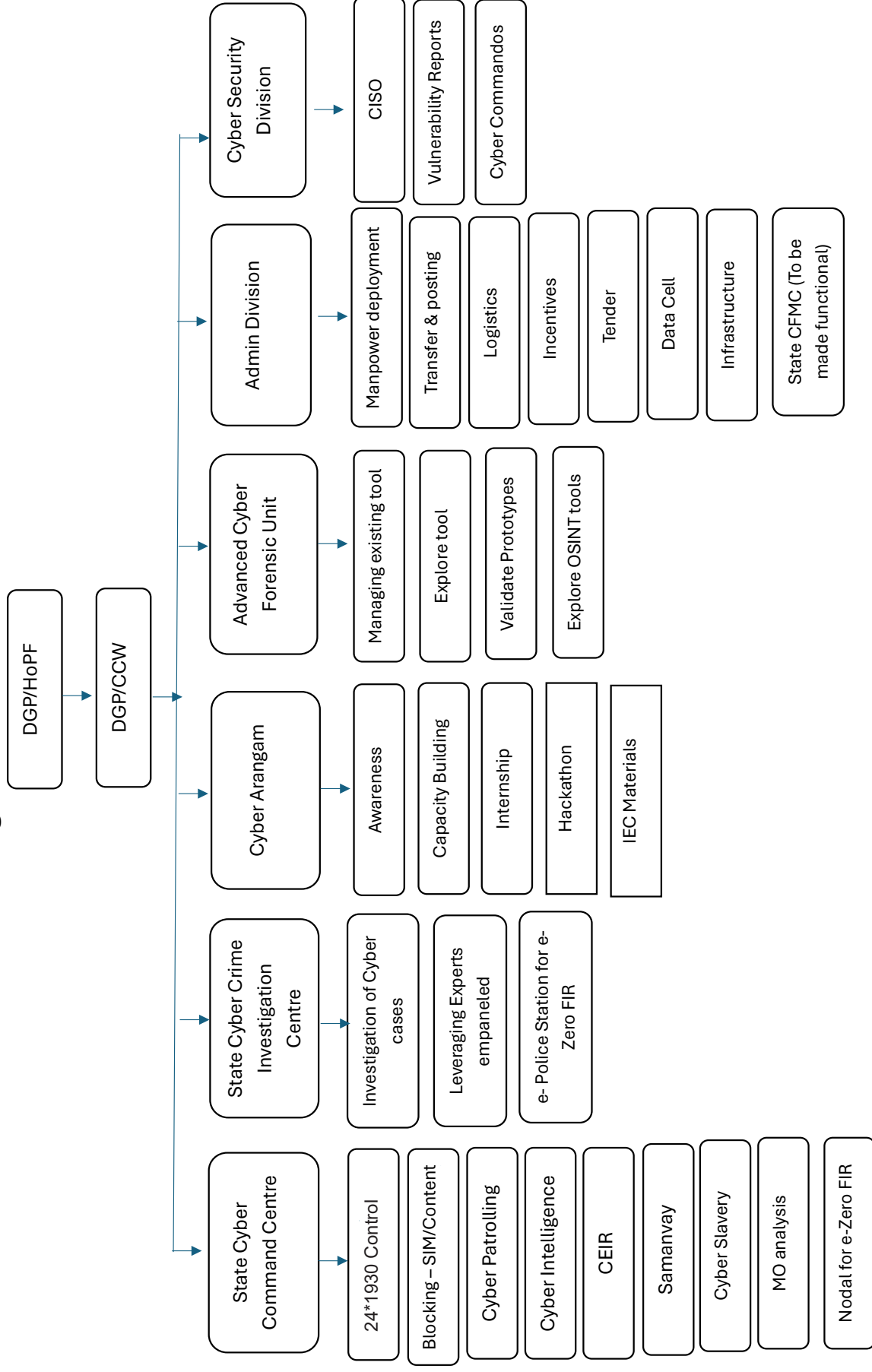
The progress and performance of Cyber Crime Police Stations shall be reviewed by the Zonal Superintendents of Police, with their concerned jurisdictional CCPS.

TN-S4C progress and functional outcomes will be reviewed by Director General of Police/TN-S4C followed by Director General of Police/Head of Police Force, Tamil Nadu on a monthly basis/ bi-monthly basis respectively.

ii) Quarterly Reviews: Progress and functional outcomes will be reviewed every three months by the Additional Chief Secretary / Principal Secretary, Home, Prohibition and Excise Department, Government of Tamil Nadu.

ANNEXURE - I

Organizational Chart of S4C



ANNEXURE – II

Staffing Pattern (Hybrid Model with subject matter experts engaged on outsourcing basis)**I. Officers:**

<i>S.No</i>	<i>Post</i>	<i>Sanctioned</i>
1	DGP, CCW	1
2	SP (CCD - I, II, III)	3
3	SP, Cyber Arangam	1
	TOTAL	5

II. State Cyber Command Centre (SCCC).

<i>S. No</i>	<i>Post</i>	<i>Sanctioned</i>
(1)	(2)	(3)
1	Deputy Superintendent of Police	5
2	Inspector of Police	1
3	Sub-Inspector of Police	20
4	Sub-Inspector of Police (Tech)	-
5	Other Rank	50
	Total	76

III. State Cyber Crime Investigation Centre (SCCIC).

<i>Sl.No.</i>	<i>Post</i>	<i>Sanctioned</i>
1.	Additional Superintendent of Police	1
2.	Deputy Superintendent of Police	5
3.	Inspector of Police	10
4.	Sub-Inspector of Police	20
5.	Sub-Inspector of Police(Tech)	5
6.	Other Rank	50
	Total	91

IV. Cyber Arangam: (OD Strength)

<i>Sl. No.</i>	<i>Post</i>	<i>Total No.of persons to be deputed on O.D. basis</i>
1	Additional Superintendent of Police (Category-I)	1
2	Additional Superintendent of Police (Technical)	1
3	Deputy Superintendent of Police (Technical)	1
4	Inspector of Police (Technical)	2

5	Inspector of Police (Taluk)	2
6	Sub-Inspector of Police (Technical)	4
7	Sub-Inspector of Police (Taluk)	4
8	Head Constable / Gr.I PC	4
9	Grade II PC	8
10	Others	1
	Total	28

V. Ministerial Staff

Sl.No.	Post	Sanctioned
1	Administrative Officer	1
2	Superintendent	3
3	Assistant	6
4	Junior assistant	6
5	Typist	5
6	Record Clerk	1
7	Office Assistant	2
8	Sweeper(BGS)	1
	TOTAL	25

Government Order Details in which above posts were sanctioned

Sl. No.	Post	Details	Total
(a)	Designation		
1.	Director General of Police	Vide G.O.(Ms).No.248 Home (Police-I) Department, dated: 22.05.2019. One post of Additional Director General of Police, created for Cyber Crime Wing, Chennai by redeploying the post of Additional Director General of Police, SID, CBCID, Chennai - Sanction Orders - Issued. Further the post was upgraded as DGP vide G.O.(Ms). No.46 Home (Police-I) Department, dated: 02.02.2026.	1
2.	SP/ CCD-I, II, III	G.O.(Ms).No.155 Home (Police-I) Department, dated: 08.03.2019, 3 posts of SP I,II & III were created by way of redeployment	3
3.	SP- Cyber Arangam	G.O.(Ms).No.223 Home (Police-I) Department, dated: 11.06.2021.	1
	Total		5
(b)	STATE CYBER COMMAND CENTRE (SCCC)		
1.	Inspector of Police	1	Proceedings of the Director General of Police, Head of Police Force in Rc.No.58789/ RA III(1)/2019, dated: 26.01.2020
	Sub-Inspector of Police-	20	
	Others	50	

2.	Deputy Superintendent of Police	5		G.O.(Ms).No.1147 Home (Police-XII) Department, dated: 01.10.2020. Redeployment of 5 Deputy Superintendents of Police to State Cyber Command Center.	5
Total					76
(c)	STATE CYBER CRIME INVESTIGATION CENTRE (SCCIC)				
1.	ADSP	1	G.O.(Ms).No.522 Home (Police-XII) Department, dated: 20.11.2021. Creation of State Cyber Crime Investigation Centre at the Cyber Crime Wing Headquarters, Chennai.		91
	DSP	5			
	Inspector of Police	10			
	Sub-Inspector of Police	20			
	Sub-Inspector of Police (Tech)	5			
	Others	50			
Total					91
(d)	MINISTERIAL STAFF				
	Administrative Officer	1	G.O.(Ms). No.492 Home (Police V) Department; Dated: 09.12.2020.		21
	Superintendent	3			
	Assistant	6			
	Junior Assistant	6			
	Typist	5			
	Record Clerk	1	G.O.(Ms). No.504 Home (Police XV) Department; Dated: 02.09.2024.		4
	Office Assistant	2			
	Sweeper	1			
Total					25

ANNEXURE – III

Budget Allocation

1. Administrative and Financial sanction to the tune of Rs.28,97,00,000/- (Rs. 23.16 crore as Non-recurring one time charges and Rs.5.81 crore as Recurring charges per year) for setting up of Cyber Police station in each districts and Commissionerates *vide* Government Order first read above. On the non-recurring fund, Cyber Crime Wing has set up state-of-the-art Cyber Forensic Laboratory at the Cyber Crime Wing Headquarters with sixteen advanced cyber forensic tools for extraction, preservation and analysis of digital evidence. Also, three important forensic tools, namely Portable Data Extraction System (MSAB XRY FIELD), Device Data Extraction Software (MSAB XRY Office) and CDR & Tower Dump Analysis System (CDAMS), have been provided to 46 District, City and Special Unit's Cyber Crime Police Stations.

2. The Government have accorded administrative sanction for a sum of Rs.11,34,56,502/- for the creation of State Cyber Crime Investigation Centre at the Cyber Crime Wing Headquarters, Chennai with the strength of 91 police personnel.

3. The Government have sanctioned an amount of Rs. 90,67,000/- under Modernisation of Police Force, State Action Plan towards "Implementation of National Cyber Crime Helpline number 1930 setup in Tamil Nadu" *vide* G.O.(Ms) No. 166 Home (Modern) Department dated: 13.04.2023.

4. The Government have sanctioned Rs.8,88,83,994/- *Vide* G.O. (Ms) No. 634 Home (Pol.12) Department dated: 19.11.2024 for 3 years towards expansion of National Cyber Crime Helpline 1930 Call Centre with 15 seaters for 3 years.

5. A sum of Rs. 20,00,00,000/- was sanctioned *Vide* G.O.(3D)No.95, Home (Police-X) Department, dated: 22.11.2024 for the construction of Cyber Crime Administrative Office Building at Police Training College Campus, Ashok Nagar in Chennai City.

6. The Government have accorded the sanction for a sum of Rs.1,00,00,000/- as recurring expenditure for Hiring of the Institutional Experts for Cyber Crime Wing and to nominate Officers for the Selection Committee to select the experts and the committee who shall decide the qualification, mode of recruitment and remuneration for the experts *vide* Government Order tenth read above.

7. The Government of India, under State Action Plan under the Scheme of "Assistance to States for Modernisation of Police" for the year 2025-26 has accorded sanction for Rs. 3,07,93,200/- *Vide* G.O. (Ms) No. 454 Home (Modern) Department Dated: 02.09.2025 for the establishment of Cyber Forensic Laboratory (Mobile Cyber Investigation Laboratory) at Cyber Crime Wing Headquarters. The following items are purchased under State Action Plan:-

Sl. No.	Name of the item & its utility
1.	Force Urbania BS VI 4400 WB (16+D) IFS [Premium vehicle to accommodate the Forensic Lab]
2.	Vehicle Customization [To setup the Cyber Investigation Lab]
3.	Digital Forensic Workstation [With high end processor to support the Forensic Tool]
4.	Tableau TX2 Imaging Tool [Images the digital evidence]
5.	Mobiledit [Mobile Extraction Tool]
6.	Oxygen Forensic Tool [Mobile Extraction Tool]
7.	Internal 3.5 HDD - 4 TB [Storage device]
8.	Standard Laptop
9.	64 GB Pen Drives
10.	DI – Forensic Card Reader
11.	Spectra Cell ID Extractor [Captures cell ID within the Tower Range]

12.	19 CDR Analyser [Does CDR and IPDR analysis]
13.	High End Laptop
14.	Multifunction Printer
15.	External 2 TB SSD (Hard Disk Advance Version)
16.	External 2 TB HDD (Hard Disk)
17.	Faraday Bag for Mobile Phone, Tablet & Laptop [Bag used to block all wireless signals to and from a device]

8. The Government of India, under Additional Supplementary Plan - II under the Scheme of "Assistance to States for Modernisation of Police" for the year 2025-26 have accorded sanction for Rs.24,08,00,000/- *Vide* G.O. (Ms) No. 79 Home (Modern) Department dated: 12.02.2026 for the establishment of Mobile Cyber Investigation Units for 50 CCPS including State Cyber Crime Investigation Centre. The following items are purchased under Additional Supplementary Plan-II:

Sl. No.	Name of the item & its utility
1.	External 2 TB HDD[Storage Device]
2.	Faraday Bag – Mobile [Used to block all wireless signals to and from a device]
3.	Force Motors Ltd Van Diesel 2596 CC[Tempo Traveller vehicle]
4.	Vehicle Customization
5.	Write Blocker[To maintain the integrity of the digital evidence]
6.	Mobiledit Forensics[Mobile Extraction Tool]
7.	I9 CDR Analysis[Does CDR and IPDR analysis]
8.	OS Forensic Pen drive[Does Live Data analysis when the system is "ON"]
9.	Tableau TX2 Tool [Images the digital evidence]
10.	Amped Five Tool[Does CCTV analysis] – only for 12 Range CCPS

9. The Government have accorded sanction for a sum of Rs.6,00,000/- *Vide* G.O.(Ms) No. 304 Home (Police-V) Department dated: 20.06.2025 for creation of 1 post of Legal Advisor for the Office of the Cyber Crime Wing on contract basis at the rate of Rs. 50,000/- per month.

10. The Government of Tamil Nadu have accorded sanction of Rs.2,10,02,831/- for creation of Dark Web in Cyber Crime Wing Headquarters, Chennai to monitor the deep and dark web, track criminal activities and perform forensic analysis of illicit online activities in the dark web vide G.O.(Ms).No.536 Home (Police-XII) Department dated: 17.10.2025.

K. MANIVASAN,
Additional Chief Secretary to Government.