Chapter III
User Management

Chapter – III

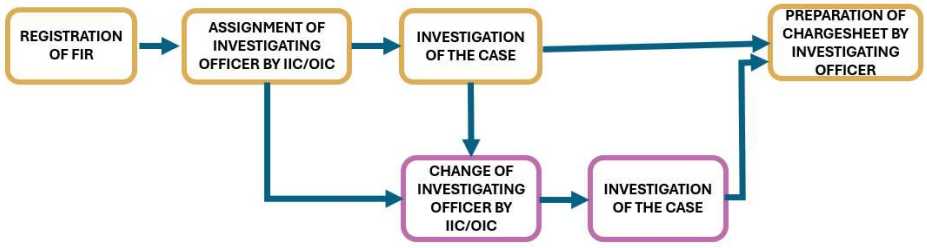
User Management

3.1 Chargesheet prepared by Officers who were not the designated Investigating Officers (IO) for the case

When an FIR is registered, the Inspector in Charge (IIC) assigns the case to an Investigating Officer (IO), who is tasked with conducting the investigation and eventually filing the chargesheet upon completion. However, in the event of the IO being transferred or assigned to a different task, the concerned IIC reassigns the case to a new IO. This new IO then assumes responsibility for continuing the investigation and ultimately filing the chargesheet.

Each IO possesses the authority to modify case details and file a chargesheet solely within the duration of their assignment to the case. However, once the case is reassigned to a different IO, the previous IO should not have access to the case within CCTNS. The intended workflow for this process is depicted below in Figure 3.1.

Figure 3.1: Flow Chart showing workflow of an FIR



For managing the assignment of a FIR to an investigating officer, the table 'FIR assign' contained Assigned IO's name for the period in which he/she was the IO of a particular FIR. Whenever there is a reassignment of the case to a different IO, a new entry is inserted into that table mentioning the date from which the new IO is in-charge of the case. In this way there is a detailed list of officers who were in-charge of different cases, and their respective periods are maintained. When an IO submits the chargesheet, the chargesheet details were

Figure 3.2: Picture showing a chargesheet by inappropriate IO

FIR No.0109

FIR reassign table

Particulars	Name of Officer	Period of assignment	
		Date from	Date to
Assignment of FIR	Suman	17 Nov 2021	27 May 2022
Re-assignment of FIR	Biswambar	27 May 2022	

Chargesheet table

On 25 May 2022, the chargesheet of the FIR was submitted by Biswambar when he was not the IO of the FIR

captured in another table 'Final Report' where along with chargesheet details the user ID of the IO and date of creation of record were also captured. Audit analysed these two tables in the database and noticed 2,080 instances across 217 Police Stations during the period from 2018 to 2023, where the chargesheet in CCTNS had been prepared by an Investigating Officer (IO) who had not been assigned to the concerned cases, as detailed below:

Table 3.1: Statement showing year-wise chargesheets filed by an officer other than the IO assigned

FIR Registration Year	Number of chargesheets filed by an officer other than the IO assigned to do so
2018	300
2019	390
2020	315
2021	635
2022	363
2023	77
Total	**2,080**

Source: CCTNS database

The above-mentioned deficiency indicated a significant control failure, as the system permitted the filing of charge sheets by personnel not authorized to do so. This carried the risk of modifications/manipulations to the chargesheets by Officers who were not the designated IOs.

Government stated (September 2024) that PS-wise specific details are being sent to concerned Superintendents of Police (SsP) for compliance and for fixing responsibility on the erring Inspectors-In-Charge (IICs) in the cases where proper authorisation was not done as per CrPC.

Despite the Government's reply, the fact remains that CCTNS still lacked necessary data validation controls to prevent such unauthorised transactions.

3.2 Unauthorised use of CCTNS credentials

Credentials, such as username and password are provided to help verify the identity of the person or entity trying to access a system. This authentication process ensures that only authorized users are granted access. By requiring credentials, a system can track and log who is accessing it. This accountability is essential for monitoring user actions and ensuring compliance with policies and regulations. Without proper authentication, unauthorized individuals or malicious actors could gain access to sensitive data or perform unauthorized actions. Credentials serve as a barrier to prevent such unauthorized access. Different users may have different levels of access and permissions within a

system. Credentials help determine what resources and functionalities each user is allowed to use. Organisations are required to comply with regulations that mandate secure authentication to protect sensitive information and maintain data privacy. Credentials are essential for managing user accounts, including creating, updating, and deactivating them. They are also crucial for user administration and security.

In CCTNS, credentials are provided from the level of Assistant Sub Inspector to the Inspector General with authorisation and specific roles to perform as per their duties. When a Station House Officer (SHO) is out of the Police Station, the following steps were provisioned be taken to register an FIR:

a. SHO could nominate a police official as In-charge (Duty Officer) during the time.
b. All the rights for SHO would be delegated to the nominated user.
c. The delegated user could register FIRs on the SHO's behalf.
d. The administrator would assign the role of SHO to the nominated person.

Test check of manually maintained leave records of employees of ten selected SP Offices and analysis of CCTNS database revealed that the credentials of Inspectors-in-Charge (IICs)/ SHOs/ IOs were used to register FIRs/ Arrests when the IICs/ SHOs /IOs were on leave, in case of 7 users on 18 occasions (***Appendix-I***). This indicated that the credentials of the IICs/ SHOs /IOs had been shared with other individuals, instead of following the approved procedure outlined above.

As login credentials are a vital control for ensuring information security and privacy, the above practice of sharing user credentials created avoidable risks. This irregular practice, coupled with the absence of application logs (as discussed in the subsequent paragraphs) resulted in inability to monitor actions taken by users in viewing and modifying data in CCTNS, and fixing responsibility subsequently.

In response, Government stated (September 2024) that the discrepancies were being sent to the concerned Superintendents of Police, with a direction to fix responsibility on the erring IICs for their lapse in not entrusting any subordinate Officer to function as In-charge of the PS through the system. However, the lack of control in CCTNS in handling cases during leave of officers and delegation of their authorities still remained.

3.3 Incorrect mapping of Police Stations with Sub-divisional Police Offices

A Sub-Divisional Police Officer (SDPO) is responsible for overseeing law enforcement activities within a designated sub-division, which is a smaller administrative unit within a district. The SDPOs are responsible for supervision of the Police Stations within their sub-divisions. To enhance the effectiveness of supervision, each Police Station was required to be mapped to the concerned SDPO, within the CCTNS.

Audit analysed the database of Police Stations mapped to SDPOs and compared the mapping in the system with the stated jurisdiction of SDPOs and observed that

- 39 Police Stations had been incorrectly mapped by SCRB to 27 SDPOs, as shown in ***Appendix-II.***
- Six Police Stations[13] had not been mapped to any SDPOs.

In response, Government stated (September 2024) that the jurisdiction of all the SDPOs as reflected in ***Appendix-II*** had been duly mapped correctly in CCTNS. It was further stated that whenever the matter of changes to the SDPO jurisdictions comes to the notice of SCRB, the mapping would be updated.

The response was not tenable, as the responsibility for updating the mapping of PSs to SDPOs had been entrusted to SCRB, but the mapping had not been updated in the cases listed in ***Appendix II***. This resulted in deficiency in effective supervision over cases in those PSs for the relevant periods.

3.4 Absence of application controls to detect duplication of data related to the same accused/complainants

One of the main objectives of CCTNS was to create a centralised crime and criminal information repository, with images and fingerprints of criminals being stored and functionalities for advanced search and retrieval of details of criminals being available.

Such functionalities would enable the police to search for persons of interest, such as persons wanted on outstanding warrants, accused of crimes, charged habitual offenders, convicts, *etc.,* across a national database. This was intended to eliminate the need for duplicate and redundant entry of data as well as the need for repetitive manual preparation of reports, thus freeing valuable time and resources for the performance of core police functions. These

[13] Ananatpur, Laxmijore, Karlapat, Manoharpur, Malkangiri Sadar and Traffic PS-2 Chandrasekharpur

functionalities would also enable viewing and exchange of information efficiently among Police Stations and other Police formations.

Audit analysed the data on criminals stored in the CCTNS database and noticed that there were instances of duplication of entries related to the same individuals (complainants as well as accused), which were identifiable on the basis of matching of data fields such as a combination of 'Name', 'Gender', 'Relative Name', 'Relation Type', 'Year of Birth', 'Address', 'Mobile No.' *etc.,* as discussed below:

Case Study

During test check of records, Audit noticed that in Jhirpani PS in Rourkela, Case No.35/2019 and Case No. 59/2019 had the same individual as accused. However, the status of the accused was depicted as arrested in one case, while concurrently, in the other case during the same timeframe, the accused was depicted as absconding. This discrepancy arose due to creation of multiple records for the same accused individual.

Multiple Records for the same accused individuals

Audit identified 10,346 instances of accused individuals having multiple records in the database. The number of multiple records created for each accused individual ranged from two to 21. Examples of such multiple records created for the same accused individual by different PSs as well as within the same PS, are shown in Table 3.2 below.

Table 3.2: Showing creation of multiple records for the same accused individual

Accused_srno	District	PS	FIR_No	Accused_name	Gender	Relative_name	Relation	YOB	Age	Address_Vill	Add_PS_cd
24503003210002246	JAJPUR	BALICHANDRAPUR	0232/2021	At** B***r*	Male	Ka***ka B***r*	Father	1985	36	Digi	24490017
24503003210002295	JAJPUR	BALICHANDRAPUR	0240/2021	At** B***r*	Male	Ka***ka B***r*	Father	1985	36	Digi	24490017
24503063210001520	JAJPUR	SUKINDA	0173/2021	At** B***r*	Male	Ka***ka B***r*	Father	1985	36	DIGI	24490017
24503069210002478	JAJPUR	KUAKHIA	0236/2021	At** B***r*	Male	Ka***ka B***r*	Father	1985	36	Digi	24490017
24490018210002219	BHADRAK	DHUSURI	0178/2021	At** B***r*	Male	Ka***ka B***r*	Father	1985	36	Digi	24490017
24503025210002144	JAJPUR	JAJPUR	0266/2021	At** B***r*	Male	Ka***ka B***r*	Father	1985	36	Digi	24490017
24503073210001403	JAJPUR	PANIKOILI	0180/2021	At** B***r*	Male	Ka***ka B***r*	Father	1985	36	DIGI	24490017
24503026210002485	JAJPUR	JAJPUR ROAD	0231/2021	At** B***r*	Male	Ka***ka B***r*	Father	1985	36	Digi	24490017
24503073210001529	JAJPUR	PANIKOILI	0163/2021	At** B***r*	Male	Ka***ka B***r*	Father	1985	36	DIGI	24490017
24503026210002754	JAJPUR	JAJPUR ROAD	0167/2021	At** B***r*	Male	Ka***ka B***r*	Father	1985	36	Digi	24490017
24490005210002537	BHADRAK	BASUDEBPUR	0225/2021	At** B***r*	Male	Ka***ka B***r*	Father	1985	36	DIGI	24490017

Source: CCTNS database

Audit noticed that such creation of multiple records for the same accused individual had taken place due to the absence of application controls to detect duplicate entry of the same data.

Multiple Records of the same complainant

Audit identified 11,711 instances of complainants having multiple records in the database. The number of multiple records created for each complainant ranged from 2 to 138. Examples of such multiple records created for the same complainant by the same PS, are shown in Table 3.3 below.

Table 3.3: Showing creation of multiple records created for the same complainant

Person_code	District	PS	FIR_No	Complainant_name	Gender	Relative_name	Relation	YOB	Age	Mobile_No	Address_Vill	Tehsil	Add_PS_cd
24491001210202671	Ganjam	Aska	0413/2021	Ra**** K***r Ch**t***	Male	Lt Pi***a** Ch**t***	Father	1977	43	6371741271	Kotagaon	jaipatana	24495017
24491001210203270	Ganjam	Aska	0495/2021	Ra**** K***r Ch**t***	Male	Lt Pi***a** Ch**t***	Father	1977	43	6371741271	Kotagaon	jaipatana	24495017
24491001210202911	Ganjam	Aska	0444/2021	Ra**** K***r Ch**t***	Male	Lt Pi***a** Ch**t***	Father	1977	43	6371741271	Kotagaon	jaipatana	24495017
24491001210203269	Ganjam	Aska	0494/2021	Ra**** K***r Ch**t***	Male	Lt Pi***a** Ch**t***	Father	1977	43	6371741271	Kotagaon	jaipatana	24495017
24491001220201567	Ganjam	Aska	0331/2022	Ra**** K***r Ch**t***	Male	Lt Pi***a** Ch**t***	Father	1977	44	6371741271	Kotagaon	jaipatana	24495017
24491001210205026	Ganjam	Aska	0813/2021	Ra**** K***r Ch**t***	Male	Lt Pi***a** Ch**t***	Father	1977	44	6371741271	Kotagaon	jaipatana	24495017
24491001210204202	Ganjam	Aska	0672/2021	Ra**** K***r Ch**t***	Male	Lt Pi***a** Ch**t***	Father	1977	43	6371741271	Kotagaon	jaipatana	24495017
24491001220201237	Ganjam	Aska	0257/2022	Ra**** K***r Ch**t***	Male	Lt Pi***a** Ch**t***	Father	1977	44	6371741271	Kotagaon	jaipatana	24495017
24491001210202912	Ganjam	Aska	0445/2021	Ra**** K***r Ch**t***	Male	Lt Pi***a** Ch**t***	Father	1977	43	6371741271	Kotagaon	jaipatana	24495017

Source: CCTNS database

Having multiple records of the same complainant can lead to data inconsistency and inaccuracies in the database. Duplicate records could lead to confusion and inefficiencies during investigations, as it would lead to waste of time and resources spent in searching for information across multiple records. It would also hinder the effectiveness of the criminal justice system by impacting case management, court proceedings, and the ability to track individuals' criminal histories accurately.

Government stated (September 2024) that steps are being taken to add provision for using existing complainants in the CCTNS which was lacking.

3.5 Absence of mandatory authentication of mobile number and/ or email address during registration of users on the Citizen Portal

When users register for a service or platform, they typically provide identification details such as their mobile number and email address for verification. This process involves sending a code (such as One Time Password, OTP) to the provided contact device/email and the user must enter this OTP to confirm access. Odisha Police's Citizen Portal offers services like Character and Employee Verification, requiring registration of users with mobile number and email address.

However, Audit noticed that the Portal had provision for users to opt for "Remind Me Later" for authentication of mobile number and email address, due to which there were avoidable risks such as creation of fake accounts and

use of bots[14] to carry out Distributed Denial of Service Attacks[15], which could result in non-availability of the system for genuine users. If the number of fake accounts was significant, it could also lead to wasted time for police personnel on verification of such users' service requests.

In reply, Government stated (September 2024) that since there had been delays in generation and transmission of OTPs to mobile numbers/ email addresses provided by users, the functionality had been provided on the Portal to complete the authentication process at a later point of time. However, the issue had been resolved and the functionality of OTP based authentication would now be implemented on the Citizen Portal.

Recommendation

Government should ensure that

- *user access management in CCTNS is compliant with business rules, so that the officers in charge are correctly mapped to roles and cases and police stations are correctly mapped to reporting authorities.*

[14] A bot is an automated software application that performs repetitive attacks over internet

[15] A Distributed Denial-of-Service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic