9. Digital Initiatives of Delhi Police

9.1. Introduction

In order to achieve the desired technological advancement to keep pace with the trends across the globe, Delhi Police has taken a number of digital initiatives during the last six years. These includes major IT projects aimed at improving efficiency of Delhi Police leveraging data analytics and latest technologies, and delivery of some services digitally through Mobile Apps and Web Applications. The records pertaining to implementation and functioning of these projects and applications were examined during the Audit and detailed observations are given in the succeeding paragraphs.

9.2. Police-centric IT Projects

9.2.1. Crime & Criminals Tracking Network and Systems (CCTNS)

Ministry of Home Affairs (MHA) conceptualized (2009) the CCTNS project as a comprehensive and integrated system for enhancing the efficiency and effectiveness of policing at all levels through creation of a nationwide networked infrastructure for tracking of crime and criminals in real time. The project involved digitization of processes and functions at all levels of policing from reporting of crime/complaint to investigation of crimes. Also, the legacy data was to be digitized and migrated to CCTNS after due validation. Primarily, MHA and National Crime Record Bureau (NCRB) were responsible for project planning, providing the Core Application Software (CAS) and project monitoring and States were responsible for project implementation including need-based customization of CAS. Delhi Police had engaged (November 2012) Tech Mahindra as System Integrator (SI) and Deloitte as State Program Management Unit (SPMU) for the CCTNS Project.

Target	**Status**
Go-Live at all locations by August 2014	Achieved in May 2016, primarily due to delayed rollout (January 2014) of the first stable version of CAS (CAS 3.0[57]) by MHA to states
CAS integration with external agencies and internal applications by July 2015	Integration with a few external agencies (e.g. Forensic Science Labs, Department of Prosecution and Department of Prisons) and applications (e.g. ZIPNET and certain modules of MV Theft and Property Theft applications etc.) was still under testing stage (September 2019) even after three years of scheduled target date.

[57] MHA rolled out the next stable version (CAS 4.5) in November 2016 and Delhi Police got its system upgraded to CAS 4.5 in September 2018.

As of July 2019, Delhi Police was using completely online version of CCTNS at 100 *per cent* of the locations and all the registrations viz. FIR, Missing person report etc. are being done on real-time basis directly in CCTNS. On detailed examination of records related to CCTNS, audit observed the following:

Issues related to Data- Migration and Quality

Data quality in CCTNS is vital since this database has to serve as the master data for police records and efficacy of any business intelligence tools shall be dependent on the quality of underlying data. There are three primary sources of CCTNS data i.e. real-time data entries at police stations, data migrated from legacy systems and data integrated from other related applications such as PA-100, MV Theft App etc.

However, it was observed that despite in-built controls like data validations, many mandatory data fields were being populated at police stations with junk data, and non-mandatory data fields[58] were left blank in spite of sufficient information available. Regarding the legacy data, the digitisation and migration of data pertaining to last 10 years (before the Go-Live date- May 2016) was reported to be complete as of February 2019. However, validation of the migrated data was still under progress at police station level and none of the police stations had completed the validation process as of July 2019. Thus, quality of legacy data was also yet to be verified. In respect of integration of database of other applications (such as MV Theft, Lost Report, e-FIR, PA-100, ERSS-112) with CCTNS, it was observed that all data fields were not being shared with CCTNS resulting in gaps in the database.

The Delhi Police, in its reply, mentions that 60 *per cent* of the migrated data has been validated by the police stations and is likely to be completed in near future. Also, the data of Register No. 9 (iii) (Data related to crime details) and Register No. 19 (Details of case property) have been validated to the extent of 100 *per cent*. Also, the data has been moved to production server.

Capacity building

– District CCTNS cells were to be created (March 2017) at each district for technical support to the operational staff, bug reporting and coordinating with the helpdesk. However, it was observed that there was lack of adequate infrastructure and dedicated manpower in the CCTNS cells.

[58] In December 2017, 25986 General Diary entries were reported blank. In case of Unidentified dead body, condition of dead body, injury marks etc. were populated with junk data

- Besides, SPMU was appointed (November 2012) for a period of three years but is still being continued (as on March 2019) as CCTNS project was yet to be completed. Meanwhile, MHA had advised (July 2017) that an incentive mechanism must be devised so that in-house personnel of Delhi Police may be motivated to take over the role of monitoring and management. However, no such initiative for incentivization was observed to have been taken by Delhi Police, which may hamper the smooth transition from consultant led project management to in-house capacity building.

Delhi Police replied (June 2020) that the SPMU Contract expired in September 2019 and an in-house team is now monitoring the project. Also, 43,611 police personnel have been trained so far for creating awareness and sensitizing them about CCTNS application.

Vulnerabilities in security architecture

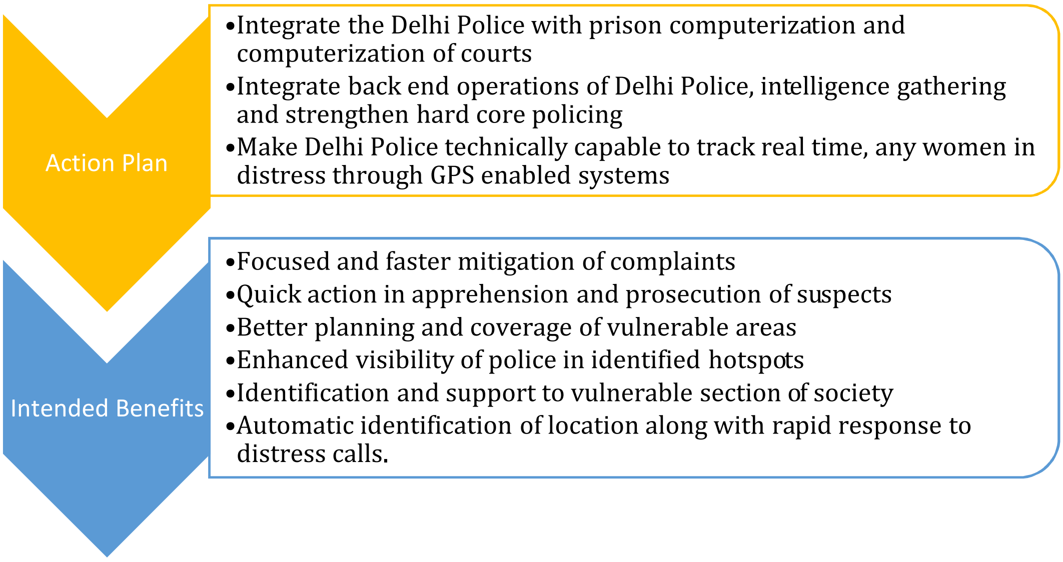
Audit further observed that a proposal for Security Operations Center was mooted (December 2016) by security expert[59] who had identified vulnerabilities in security architecture of CCTNS. However, decision in respect of the proposal was pending as of August 2019. Also, third party audit of CCTNS again highlighted (June 2019) critical vulnerabilities of CCTNS, which primarily hinted at an ageing system and outdated nature of applications/software being used.

Delhi Police replied (June 2020) that a proposal for Technical refresh has been prepared and is under consideration currently.

9.2.2. Safe and Secure Delhi

The Ministry of Home Affairs proposed (January 2013) to Ministry of Electronics and Information Technology (MeitY) a project titled ‘Safe & Secure Delhi’ under World Bank funded ‘e-delivery of Public Services projects’ with intended benefits as given in Picture below:

[59] Security Expert was hired in SPMU team for 3 months w.e.f. 8/02/2016, with a mandate to comment on security aspects for data center and various applications. In terms of cyber security maturity level, the report rates Delhi Police at a primitive, “Stage 1” out of 5 graduated levels.



Action Plan

- Integrate the Delhi Police with prison computerization and computerization of courts
- Integrate back end operations of Delhi Police, intelligence gathering and strengthen hard core policing
- Make Delhi Police technically capable to track real time, any women in distress through GPS enabled systems

Intended Benefits

- Focused and faster mitigation of complaints
- Quick action in apprehension and prosecution of suspects
- Better planning and coverage of vulnerable areas
- Enhanced visibility of police in identified hotspots
- Identification and support to vulnerable section of society
- Automatic identification of location along with rapid response to distress calls.

The project cost was estimated (January 2013) at ` 40 crore[60] in two phases over a period of 12 months. The MeitY conveyed Administrative Approval (AA) for ` 14.75 crore in July 2013 and acceptance of the terms and conditions of the AA was conveyed back by Delhi Police after 10 months in May 2014. To guide and review the progress of project implementation, MeitY constituted a Project Review and Steering Group (PRSG) which subsequently recommended (November 2017) for closure of the project citing "*Undue delay in finalization of System Integrator by the Delhi Police*".

The project mainly comprised of the following components and activities:

- Linking all existing Databases of various Delhi Police Units for seamless real-time exchange of information (Enterprise Information Integration Solution - EI2S)
- Collate, categorise, analyse and convert unstructured information into meaningful and actionable intelligence (Open Source Intelligent Solution - OSINT)
- Delivery of required information '*on the move*' to various stakeholders via Mobile terminals and interactive PDAs

The consequence of the failure of the project (and avoidable loss of grants amounting to ` 40 crore) was that IT projects of Delhi Police continue to be siloed, disparate, and not linked.

[60] Phase-I of ` 14.745 crore and Phase-II of ` 25.285 crore.

9.2.3. Safe City Project

The MHA conceptualised (November 2017) the 'Safe City project', aimed at safety for women in public places in eight metro cities including Delhi. The project was to be funded by Nirbhaya Fund and proposals were to be submitted by Police Commissioners and Municipal Commissioners by December 2017.

Delhi Police submitted (November 2017) a detailed project proposal report 'Women Safety-CCTV surveillance in public places' to GoI with preliminary estimates for ` 1250 crore and key components of 24x7 CCTV surveillances of places frequented by women or prone to women related crime, Integration of location based services and crime and criminal databases with CCTV feeds, real time video analytics and generation of actionable alerts. The project proposal was later revised to ` 858 crore and approved (February 2019) by the Government of India with directions that Delhi Police, in consultation with Line department of Ministry of Women and Child Development, GoI, Govt. of Delhi, NCR and other stake holders, shall prepare non-technological community led interventions, and shall ensure convergence with similar projects by other agencies.

Audit observed that unlike the proposals for other metro cities, the proposal of Delhi Police did not include any non-technological component such as community policing, soft skill training, induction of women in police etc. and it was surveillance-centric despite the fact that existing cameras installed by Delhi Police were not functioning properly (discussed in Paragraph 6.3.1).

It was also observed that Delhi Police had initiated proposal (September 2016) for a study[61] on crimes against women but the study could not be conducted till September 2019. Besides, no impact assessment study has been conducted by Delhi Police for the effectiveness of already installed cameras in prevention of crimes, especially against women.

Thus, in the absence of any substantiated study on efficacy of surveillance in preventing crime or impact assessment study for existing cameras, heavily surveillance centric project of Delhi Police needs to be reviewed. Project proposals of other metro cities were much comprehensive with combination of surveillance system, patrol vehicles, road lighting, emergency call boxes, social

[61] Sociological study on causes of rape and psychoanalysis of rape accused

media abuse tracking, legal assistance, behavioural change campaign, gender sensitisation, impact assessments etc.

The Delhi Police replied (June 2020) that many non-technological / community-led initiatives were also being taken by the Police. It was further replied that work order to start survey for implementation of the project was awarded to Centre for Development of Advanced Computing (C-DAC), Pune as Total Service provider in September 2019. As of June 2020, the detailed project implementation Plan submitted by C-DAC Pune in May 2020, is under consideration by the Technical committee.

Delhi Police may consider commissioning a third-party evaluation of these initiatives so as to ascertain the efficacy/ impact assessment of surveillance-based policing.

9.2.4. CMAPS (Crime Mapping, Analytics and Predictive System)

Delhi Police and Indian Space Research Organisation–Advanced Data Processing Research Institute (ISRO-ADRIN) had signed (December 2015) an Memorandum of Understanding (MoU) to develop CMAPS, i.e. a web-based application deployed in Delhi Police Headquarters and accessible via a browser from all police stations and districts of Delhi. It was primarily envisioned as a Decision Support System for Police. The major function of CMAPS was to spatially map the crime types, analyze the crime related data based on various parameters (region, frequency, crime type etc.), so as to gain a better insight into criminal behaviour which helps control it.

ADRIN was responsible for development of application, analytical tools and techniques whereas Delhi Police was responsible to provide the hardware, infrastructure, capacity building costs and data for the system. The project was to be completed by December 2018 in four phases with a graduated level of features i.e. Crime analytics module, Security module (target threat rating, situation database creation), News Module (Geo tagging, clustering) and Social media and siterips (Social network analysis, Text annotation). Audit, however, observed that CMAPS largely fetches data from PA-100 only and complete integration with CCTNS was yet to be achieved (as of September 2019), which could have enabled better utility owing to wider profile of data available. Also, the advanced features like security module, open source content analysis (from News and Social media), etc. have not been implemented.

Meanwhile, Delhi Police and ADRIN had deliberated (November 2017) upon some incremental features e.g. criminal profiling and analysis, mobile based CMAPS etc. to be implemented by January 2018. However, no progress was made in this regard either and records made available to audit did not indicate any communication by Delhi Police with ADRIN after March 2018.

Regarding the capacity building among the key stakeholders i.e. officials responsible for decision making, Delhi Police requisitioned (March 2018) CDAC to arrange training program for Constables and Head constables. However, training to Constables and Head constables lacks justification since CMAPS is to be used by senior management to aid decision making while effecting changes in deployment, recalibration from active policing to community policing, generating actionable intelligence etc. and training of lower constabulary for CMAPS might not be useful. Besides, lack of appreciation of technology was evident in this project as well, as all the four phases were projected to be completed within 12 months while remaining time was allocated for MoU finalisation, problem formulation etc.

Thus, IT projects were ill-planned as the timelines committed were unrealistic e.g. in Safe and Secure Delhi project and were inadequately monitored as seen in CMAPS, which witnessed diminished interest after initial stages.

Delhi Police should implement the IT projects in an iterative manner with staggered timelines and sufficient gaps for learning and feedback from user units.

9.3. Citizen-centric service delivery applications

9.3.1. Himmat/Himmat Plus App

Himmat (later upgraded to Himmat Plus) is a women safety centric mobile application of Delhi Police, which provides the functionality of sending SOS to Police control room, along with the location coordinates of distress caller. Himmat App was initially launched by Delhi Police in January 2015. The app development cost incurred was ` 45 lakh and ` 4.5 lakh were spent annually on AMC (Annual Maintenance Contract) for 3 years. The Himmat App was later replaced with Himmat Plus in February 2018. The cost of development of Himmat Plus was ` 18.5 lakh and cost for AMC is ` 2.77 lakh plus taxes. Thus, the total expenditure incurred on development and AMC for Himmat/Himmat Plus App was ` 83.5 lakh (as on August 2019). Audit observed the following issues related to development, adoption and publicity of the Application:

Development of Himmat and Himmat Plus Mobile Apps

- Ideally, an application should be developed on basis of user requirements and calling for the proposals from prospective firms. As per the records, the user requirements were broadly mentioned and file notings stated that after a market survey, only 'Smartcloud Infotech' (firm) was found to meet the requirements. Accordingly, the Himmat app was purchased (December 2014) from 'Smart Cloud Infotech' (firm) on nomination basis without calling for quotations or proposals from any other prospective firms.
- Further, PHQ raised certain queries regarding issues such as cost, proprietary nature of the solution and past experience of implementation by the firm. However, the Unit concerned (Ops and Communications) sought replies for queries from the firm ('Smart Cloud InfoTech') itself and forwarded the replies received from the firm to PHQ.
- Although Delhi is predominantly Hindi speaking region, Himmat App was launched only in English language, and was made Bilingual (Hindi and English) after more than two years, i.e., in April 2017. This was on behest of parliamentary Committee on Home Affairs, which mentioned (March 2017) that the lack of Hindi language support might be responsible for low downloads.
- Later, Himmat Plus App was launched (February 2018) as a new application instead of updating Himmat App. Regarding this, as per the records made available, there was no deliberation on whether the Himmat App should have been updated or an entirely new Application was required. Moreover, records made available did not indicate any efforts to reach out to the users of Himmat App and to ensure that they migrate to Himmat Plus. There was a possibility that existing users of Himmat App might not have moved to Himmat Plus.

The Delhi Police, in its reply (June 2020), mentions that before the finalization of Himmat application, comparative evaluation of apps by Tech Mahindra, CDAC etc. was carried out. However, the supporting documents have not been furnished to audit. Also, a mention has been made of the field-testing report of the app, in various parts of India with support of local police, prior to installation. However, the field-testing reports have not been provided to audit.

- Delhi Police did not discover costing for the application on its own, and rather accepted the costing model (‘Nil’ base cost and ` 1.5 lakh per console) offered by the firm i.e., ` 45 lakh for 30 consoles.

  Moreover, since the costing model was based on consoles, assessment of exact number of consoles required should have been done. However, the records did not indicate any assessment to arrive at requirement of 30 consoles. This is despite the fact that MHA’s approval was conditional on the “requirement of 30 consoles being a bare minimum to achieve the intended objective” Surprisingly, the quantum of calls on Himmat helpline did not justify more than two consoles. It indicates requirement of consoles was not assessed properly and was heavily based on developers’ suggestions.

Delhi police replied (June 2020) that the 30 consoles included 10 call taker positions earmarked for Women Helpline (WHL) and 20 dispatcher positions who dispatched the PCR Vehicle. The call taker used to generate challan on PA-100 system. The reply is not satisfactory as the consoles at 20 dispatcher positions were sparingly used as indicated by the status of challans generated remaining ‘Open’ (final action not taken at Dispatcher console of Himmat App).

- The “Terms and Conditions” as per the installed Himmat Plus app mentions that the underlying software code are owned by Delhi police. Audit, however, observed that no license or source code has been provided by the firm to Delhi Police.
- The detailed project proposal by the firm mentions features like- “Analytics report for the police personnel to identify risk areas, demographics”, “personnel app and patrol vehicle app” which were never provided, as verified by audit.

Delhi police replied (June 2020) that they are taking up the matter with the firm to know the amount involved in not providing these functionalities and said amount would be recovered from the firm. The reply is not satisfactory as Delhi Police should independently assess the amount that would have been incurred had these functionalities developed.

- As per the Security Audit Reports of the App, certain vulnerabilities were pointed out e.g. unencrypted storage which can lead to data theft, insufficient transport layer security leading to risk of packet sniffing on an unencrypted channel, risk of SQL injection, clipboard vulnerability etc.

However, these were mentioned as a business exception without sufficient justification.

Delhi Police may ensure that the vulnerabilities are resolved immediately since the Himmat App data also contains videos recorded by mobile phones, which may lead to privacy issues in case of leakage.

Delhi Police replied (June 2020) that prima facie, there was no need for encryption as the data was migrated to National Informatics Centre (NIC) servers after 2017. However, the need for encryption was being discussed with vendor and would be implemented if needed. Though the encryption issue is being taken up with vendor, the reply is not satisfactory as the migration of data on secure NIC servers does not per-se solve all the security issues. In the opinion of audit, other security protocols like Transport Layer Security must be instituted at the earliest.

Installs and usage of Application

– There were total 1.01 lakh Installs for Himmat App and 0.65 lakh installs for Himmat Plus App (till May 2019) i.e. a total of 1.66 lakh till May 2019, on Google Android platform. However, there were 1.32 lakh uninstalls as well during the same period. This indicated poor user retention as 80 *per cent* of the users uninstalled the app after installing the app.

  Further, out of the 0.34 lakh remaining users, only 16,557 users have opened the Apps at least once in last 30 days (as on 16th May 2019).

– Regarding the ride sharing feature in Himmat Plus app, on scanning the QR Code displayed in a Taxi, the driver and taxi details are shared with Delhi Police and user can press SOS button in case of emergency. However, the QR codes are installed in only Black & Yellow Taxis and Airport Cabs, and does not include the Cab Aggregators (Ola, Uber etc.).

  As on May 2019, only 4303 drivers were registered with Himmat QR codes. Thus, absence of QR codes in Cab Aggregators has rendered this whole functionality deficient and it is indicated in poor usage of this function by users (3393 scans by users till May 2019).

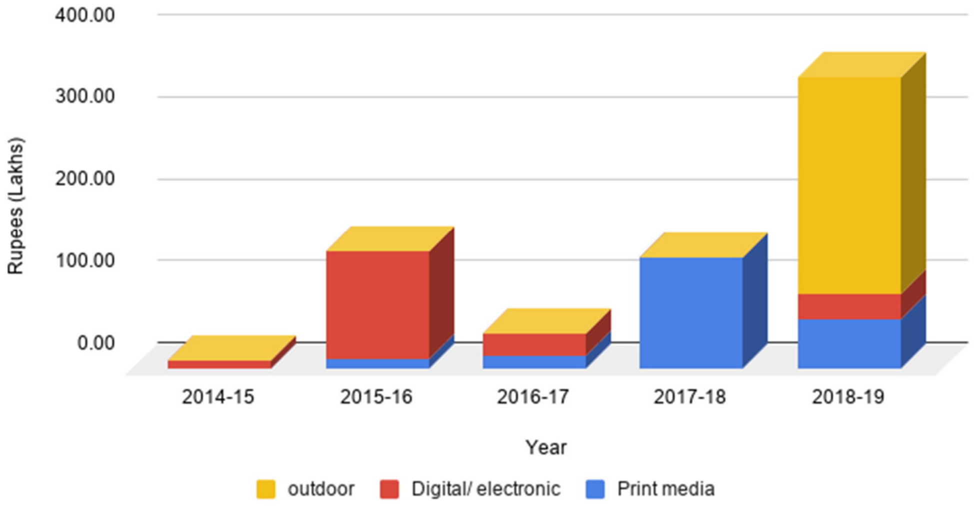
– Since the introduction of Himmat App in January 2015 till May 2019, 442 actionable calls were generated through SOS feature of Himmat and Himmat Plus Apps, and a total of 9 FIRs were registered.

  As per the Delhi Police reply (June 2020), 827 number of actionable calls and FIRs has increased to 827 and 10 respectively. The number of actionable calls when seen against the 75,032[62] crimes against Women reported during the same period of 1st January 2015-15th June 2020, indicates a dismal picture.

Publicity of Himmat and Himmat Plus Applications

Delhi Police has incurred total expenditure of ` 6.82 crore on advertisements (print, electronic and outdoor) for Himmat and Himmat Plus during last five years from 2014-15 to 2018-19 (Chart 9.1). However, such aggressive promotion has not translated into any palpable increase in user retention/ wider adoption, except at the launch of Himmat and Himmat Plus apps.

Chart 9.1: Advertisement Expenditure on Himmat/ Himmat Plus App

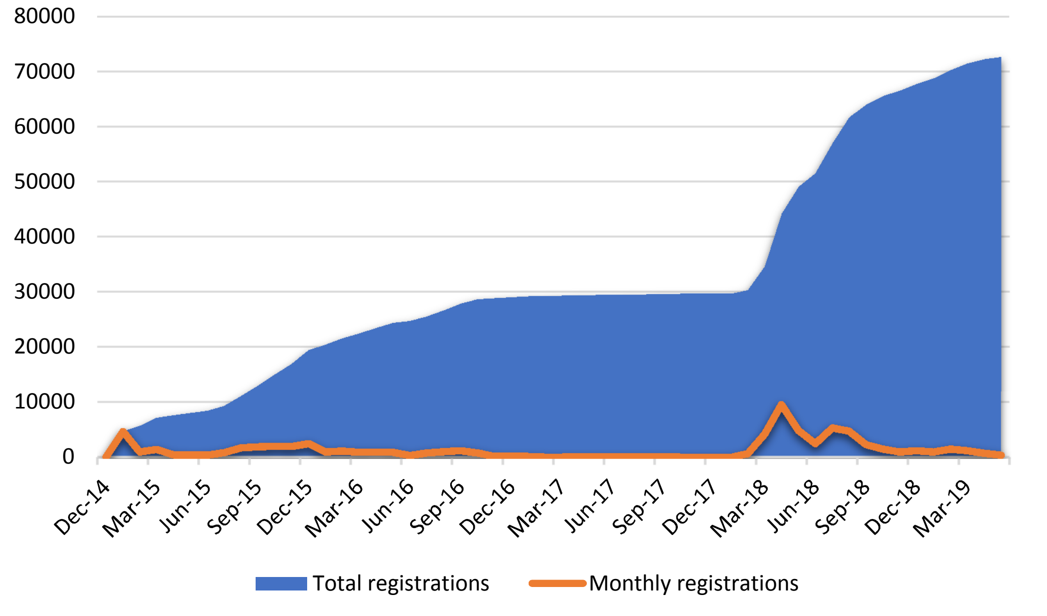


Source: Information provided by Delhi Police

The pattern of registration in Himmat and Himmat Plus Apps during the period from December 2014 to March 2019 is depicted in Chart 9.2.

[62] As per the Statistics on Delhi Police Website.

Chart 9.2: Registration in Himmat and Himmat Plus Apps



Source: Information provided by Delhi Police

It is evident from Chart 9.2 that user registrations spiked at the launch of Himmat App (January 2015) and then at the launch of Himmat Plus App (February 2018), and the surge in advertisement costs in 2015-16 and 2018-19 did not have a long-lasting impact, while advertisements in 2016-17 and 2017-18 had minimal impact.

Comparison with similar apps by other state Police.

Himmat application, its features, performance, user adoption and incident costs were compared against those of similar apps launched by different state Police departments in Haryana, Bengaluru and Maharashtra.

	Delhi Police (Himmat/Himmat Plus)	**Bengaluru Police (Suraksha)**	**Maharashtra Police (Pratisaad)**	**Haryana Police (Durga Shakti)**
Launched in	January 2015	April 2017	January 2016	July 2018
Development cost + AMC	` 83.5 lakh	NA	NIL (as a CSR initiative)	` 0.50 lakh
Installs (till May 2019)	` 1.66 lakh	` 1.03 lakh	` 1.50 lakh	` 1.33 lakh
Current Users (May 2019)	33,000	50,482	84,000	34,000
Advertisement costs	` 6.82 crore	` 0.98 lakh	NIL	` 8.8 lakh
Actionable Calls (till May 2019)	442	4885	NA	852

It was observed that the Personal Safety applications of other states had a greater number of installs and actionable calls, less cluttered user interface, and almost negligible expenditure on publicity due to massive use of social media.

Delhi Police spent about seven crore rupees in the last four years on promotion via the traditional media (electronic, outdoor, newspaper), which has not translated into proportionate gains in terms of app installs and usage.

This is evident in the poor retention rate (almost 80 *per cent* of the users uninstalled the app), meagre number of actionable calls (SOS Alerts) received, and high per client acquisition cost of ` 2,320[63] to the Delhi Police. It is also evident from the fact that as against 75,032 crimes against women reported, only 827 SOS Alerts through the App were received during the period of January 2015-June 2020.

Delhi Police should examine why their Himmat/Himmat Plus App has failed to provide the intended benefit, inspite of the crores of rupees spent on its development and publicity.

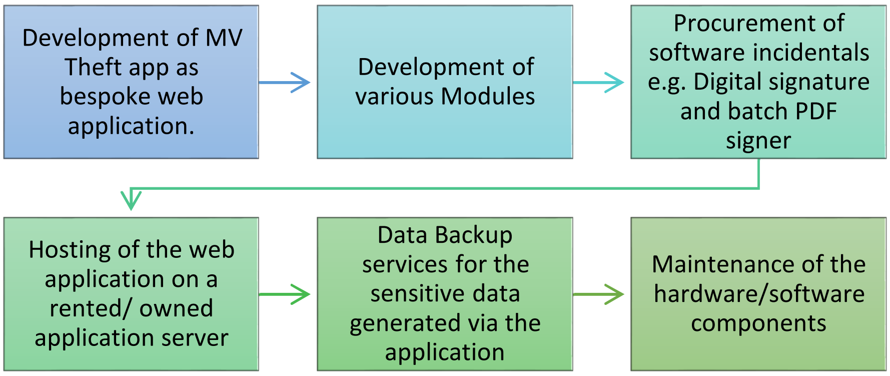
9.3.2. MV Theft App (Motor Vehicle Theft Application)

Delhi Police developed this application (web and mobile) to ensure trouble free registration of e-FIR of Motor Vehicle thefts, automated investigation and electronic generation and transmission of final report for online acceptance by the competent e-Court. Within 24 hours of generation of the e-FIR, Investigating Officer (IO) is assigned, who then contacts the complainant and conducts the investigation. The application delivers printable digitally signed Untraced Report to the complainant to process the insurance claim. Audit observations related to development and functioning of MV Theft Application are detailed in the succeeding paragraphs:

Development of MV Theft Application

The development of MV Theft web application was initiated in September 2014. The entire process can be broken down as:

[63] Per user Cost=Total cost/Total No. of users; Total cost = ` 6.82 crore (advertisements) + ` 0.835 crore (development + AMC); No. of users: 33,000.


Development of MV Theft app as bespoke web application.
Development of various Modules
Procurement of software incidentals e.g. Digital signature and batch PDF signer
Hosting of the web application on a rented/ owned application server
Data Backup services for the sensitive data generated via the application
Maintenance of the hardware/software components

Audit observed following irregularities in the award of above works:

- For a coherent web application development, it is desirable that all the functional modules for software are identified by the agency/bidder, at the outset, and price bid be called/quoted for the entire package (with staggered timeline for modules, if required). This would enable hassle free implementation and also fair price discovery. Contrary to this, it was observed that unrelated bids were invited for six different components of a single web application. However, all the bids were ultimately awarded to a single firm (M/S PC Solutions).
- Delhi Police invited (September 2014) bids for development of the MV Theft Application (Core component of the MV Theft application package) and out of three bids received, the lowest bidder i.e. M/s PC Solutions was awarded (January 2015) the work at a cost of ` 1.98 lakh.
- Delhi Police invited bids for development of DO (Duty Officer) module of the application on 30th October 2014 i.e. even before the work for development on core component was awarded.
- Further, bids for development of three modules i.e. IO (Investigating Officer) Module, Court Module and MIS Module, were invited on the same date (14th March 2015) and awarded on the same date (31st March 2015) to M/s PC Solutions. It is important to note that Delhi Police verified the completion of work of all the three modules on the same day itself, which was not feasible.

Table 9.1: Details of MV Theft Application and its modules

Particulars	Tenders/Quotes invited on	Awarded to	Awarded on	Awarded at	Implemented on
MV Theft Application	29.09.2014	M/s PCS	27.01.2015	` 1.98 lakh	10.03.2015
DO Module	30.10.2014	M/s PCS	27.01.2015	` 1.99 lakh	10.03.2015
IO Module	14.03.2015	M/s PCS	31.03.2015	` 1.99 lakh	31.03.2015
Court Module	14.03.2015	M/s PCS	31.03.2015	` 1.99 lakh	31.03.2015
MIS Module	14.03.2015	M/s PCS	31.03.2015	` 1.99 lakh	31.03.2015
STA Module	June 2016	M/s PCS	26.07.2016	` 0.99 lakh	26.08.2016

Source: Compiled from records of Ops & Comm Unit, Delhi Police

- Delhi Police had purchased (November 2014) two digital signatures and pdf signing software for MV Theft App. Audit observed that the digital signatures and pdf signing software were handed over to M/s PC Solutions on 28th November 2014 i.e. two months before the issue of work order for development of Application to M/s PC Solutions on 27th January 2015.
- Delhi Police, on basis of market survey, hosted (November 2014) the application on rental server provided by M/s PC Solutions at ` 41,465 plus taxes per month. Since the initial proposal was to use rental server for only two months, Delhi Police had resorted to market survey only to identify the lowest rate. However, Delhi Police ended up using the server for 34 months (till September 2017) at cumulative cost of ` 14.10 lakh plus taxes without resorting to proper price discovery through tendering. Further, no efforts were made to renegotiate the rental cost considering the trend of declining price for hosting services. Similarly, Delhi Police took cloud backup services from M/s PC Solutions from August 2016 till August 2017 at total cost of ` 6.29lakh on basis of market survey.

The above observations point towards an irregularity in the process of planning for app development and a violation of procedure for inviting bids to enable fair price discovery. Ultimately all the 13 works related to MV Theft were awarded to M/S PC Solutions through unrelated bids at cumulative amount of ` 44.50 lakh.

Functioning of MV Theft Application

- The Mobile application for MV Theft remained functional from April 2015 to May 2017, after which the application was removed from google-play store for non-compliance with End User License Agreement (EULA) and had not been reinstated since. Thus, only the web version of MV Theft Application was available since May 2017.
- The website for MV Theft application was not secure as the communication between web clients and server is not secured using the HTTPS protocol. Thus, there is a need to encrypt the data in transit using any transport layer encryption service (TLS/SSL) which ensures the authenticity of website and encrypts the communication.

  The Delhi Police, in its reply (June 2020) mentioned that the SSL certificate had been procured and implemented. Audit, however, verified (July 2020) that the SSL certificate was still not available for MV Theft App.

- On analysis of data dump, audit observed instances of multiple FIRs registered against theft of the same vehicle. The application should not allow registration of multiple FIRs against vehicles with the same registration number since it not only results in overstatement of theft cases, but also results in wastage of resources. Audit also observed seven entries with duplicate FIR number, reasons for which could not be ascertained.
- There were poor data validation checks while filling online form for registering FIR on the web application e.g. special characters were accepted in 'Name', Date of birth does not have any limiters and even a future date was being accepted, etc. such lack of validation checks adversely affects the data quality of application and other linked systems and limits its utility for generating actionable information.

Delhi Police's reply (January 2020) mentions that the lacunae regarding data validation has been noted and is being rectified in the application.

9.3.3. Other applications

Besides Himmat/Himmat Plus App and MV Theft App, records pertaining to the following five web-applications of Delhi Police were examined during the audit.

Application	Details
Property Theft App	To ensure trouble free registration of e-FIR for cases involving only theft of some property
Lost Report App	To enable reporting of any lost/missing articles (documents, credit cards etc.) without the need to go to a police station, and a printable digitally signed report is instantaneously sent in response to the complainant.
Found Articles App	To get updates regarding the article reported as lost/missing in 'Lost Report' Application, and for reporting of some article/document found by any person
Police Clearance Certificate App	To apply for PCC, required by an individual while applying for employment in private sector and for emigration purposes
Character verification Report App	To enable online applications from employers[64] for verification of character and antecedents of their employees

Audit observed the following deficiencies in the development and functioning of these web-applications:

- It was observed that similar to MV Theft App, the Property Theft App and Lost Report App were developed in two phases each even though both the phases were initiated at the same time and splitting of the development work was not justified.

[64] On payment basis for private employers

- Similar to MV Theft App, all the above five web-applications were also not secure as the communication between web clients and server was not secured using the HTTPS protocol. Also, there were poor data validation checks while filling online form for registering FIR on these web applications as well.

  Delhi Police replied (June 2020) that SSL certificate has been implemented and data validation checks are already in place. On verification (July 2020), audit found that SSL certificate was not available for Property Theft App, Police Clearance Certificate App and Character Verification Report App. Similarly, data validation issues were also still present in the applications (July 2020).
- The 'Found' Application was not functioning as the OTP required for registration of user was not received on multiple attempts during May-September 2019.

  Delhi Police replied (June 2020) that OTP can be received via email if not received by phone number. Audit, however, verified (July 2020) that OTP was not received for 'Found' application, and instead an Error page appeared.

9.4. Imperative for a Comprehensive IT Policy

Delhi Police has an IT cell and a temporarily appointed Chief Technology Officer, albeit without any dedicated staff. The IT Cell has only 25 persons in position as against a sanctioned strength of 52 personnel. Moreover, the IT cadre is not structured according to the demands of modern IT management. Lack of a dedicated IT policy to handle issues like framing of guidelines, granting centralized approval, deciding technical specifications, further compounds the problems. An IT perspective policy/ Framework is also desirable to account for a growing organization, with constantly increasing reliance on Information Technology.

In the last few years, there has been a spurt in the acquisition of IT assets by all Delhi Police units, ranging from Computer Aided Dispatch and web/mobile applications to surveillance systems. This has led to increased opportunities for technology/ data driven policing as well as threats (Data security, network security etc.). This necessitates a comprehensive IT policy to address some extant issues, as below:

- **Lack of adequately skilled personnel**: In-house skill level in Delhi Police is low owing to the severely limited strength of IT cadre. The personnel trained by vendors (e.g. for PA-100, CCTNS) were not sufficiently incentivized to develop skills further. Moreover, the functional roles for staff keeps on changing according to unit of posting.

  Delhi Police need to induct IT professionals and incentivize the in-house trained manpower to reduce dependence on vendor/ consultant for system/network administration, minor customizations etc.

Delhi Police replied (June 2020) that rank based vacant posts will be filled in due course and restructuring of posts is also in the process. The Government has replied (July 2020) that Delhi Police should have regular post of IT head/Chief technology Officer who can have complete knowledge and understanding of IT infrastructure and assessed requirements according to functionality of IT cell. It has further stated that Delhi Police should have sufficient technical and trained manpower to run its IT cell securely, smoothly and efficiently.

Audit is of the view that Government and Delhi Police together take necessary steps to ensure that IT skills of Delhi Police personnel is enhanced and IT systems of Delhi Police runs efficiently.

- **Regular monitoring of the progress of IT asset**: Different Delhi Police units are pursuing projects in un-concerted manner, without defined timelines for completion, and agreed upon functionalities, creating systemic inefficiencies[65]. Thus, a comprehensive IT Policy with defined (SOPs for various kind of IT projects and a centralized dashboard for monitoring the progress and implementation strategy of IT projects is desirable.

Delhi Police replied (June 2020) that the projects are monitored by the user unit, and monitored by senior officers. The reply is not satisfactory, as it is imperative for Delhi Police to monitor the progress of its IT projects in a more efficient way, since all the projects suffered from delays and lack of regular supervision and monitoring.

The Government has replied (July 2020) that Delhi Police being a sensitive organisation, should have Information/Cyber Security Policy which should cover security aspects. The reply is silent regarding action taken in this regard.

[65] Example- Disparate web applications, with dedicated infrastructure, the data of which is to be ultimately transferred to a Centralized (CCTNS) system is needless, when the same thing can be implemented on a common infrastructure, without the need for data migration at later stage.