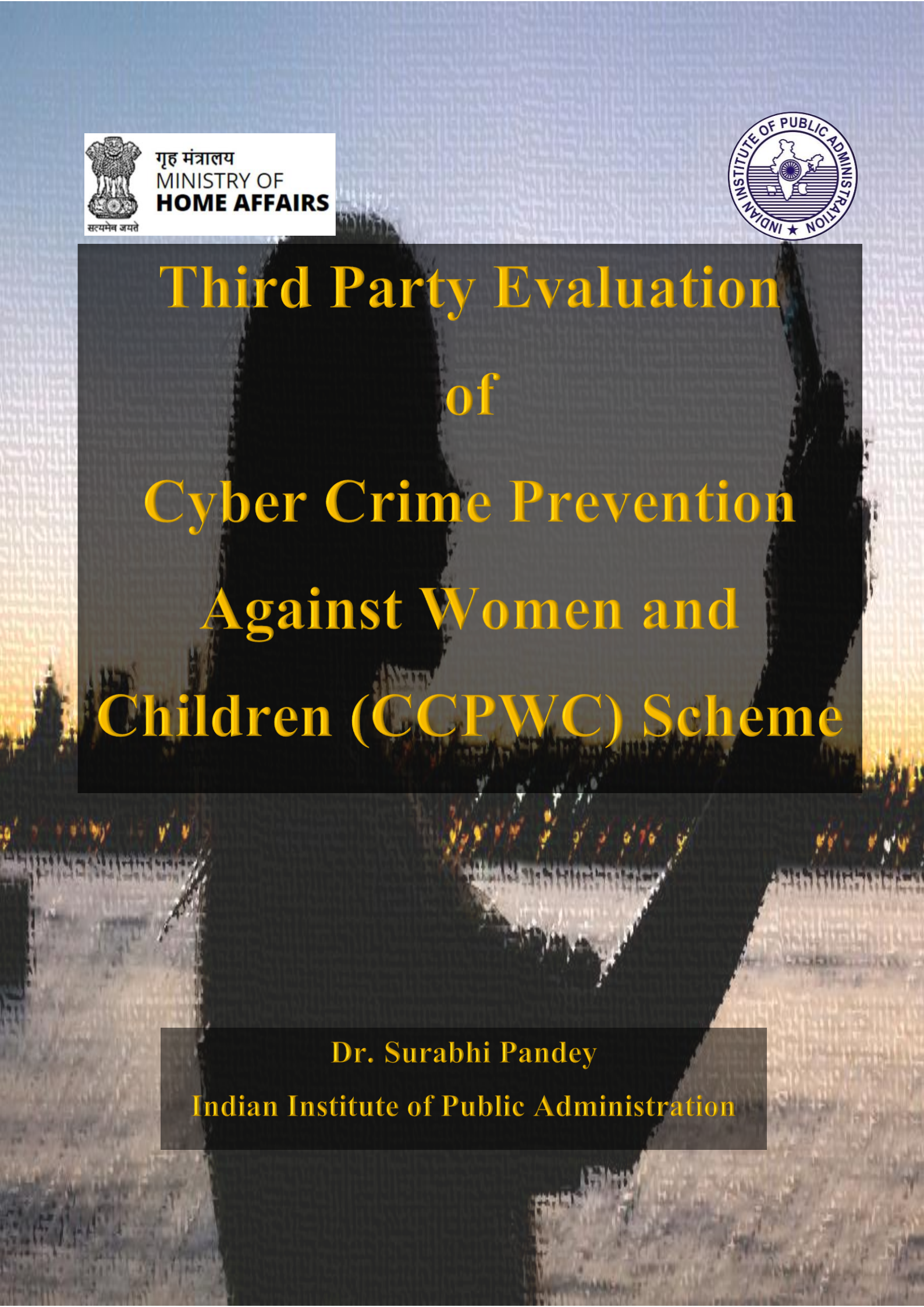


गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
सत्यमेव जयते

Third Party Evaluation of Cyber Crime Prevention Against Women and Children (CCPWC) Scheme

Dr. Surabhi Pandey
Indian Institute of Public Administration

Report on

Third Party Evaluation of Cyber Crime Prevention Against Women and Children (CCPWC) Scheme

Project Head

Dr. Surabhi Pandey

Research Team

Ms. Munisha Chauhan

Mr. Shaurya Singru

Sponsored by

Ministry of Home Affairs

Government of India

Conducted by

Indian Institute of Public Administration

New Delhi- 110002

2021

Acknowledgement

We express our deep gratitude and thanks to the Cyber and Information Security (C&IS) Division, Ministry of Home Affairs, Government of India, for entrusting IIPA with the assignment of conducting Third-Party Evaluation of Cyber Crime Prevention Against Women and Children (CCPWC) Scheme.

We express our special thanks to Shri. Ashutosh Agnihotri JS (CIS), Shri. Praveen Kr. Yadav DS (CIS-III/Parliament), Shri. B L Meena US (CIS-II), Shri. K. L. Budhiraja, and Shri. K.J. Sunny SO (CIS-II) of the MHA for providing their generous support and cooperation throughout the study.

We are also grateful to the Nodal officers of the implementing agencies and stakeholders under the scheme for cooperating with the IIPA study team and providing all the required data and insights.

Special thanks to Shri Amitabh Ranjan, Registrar, IIPA for his guidance and extending all administrative support throughout the project.

Sincere thanks to Dr. Surabhi Pandey, Assistant Professor, IIPA for the excellent execution of the project study.

Finally, thanks to Account Section of IIPA, Shri Jaswant Singh, Liaising Officer, and the Research Team: Ms. Munisha Chauhan, Research Officer and Mr. Shaurya Singru, Research Associate for constantly assisting, as well as sincerely sharing all the responsibilities involved in the timely conduct and completion of this study.

Shri. S N Tripathi IAS (Retd.)
Director General , IIPA

Table of Contents

List of Tables

List of Graphs

List of Figures

List of Abbreviations

BPR&D	Bureau of Police Research and Development
CCPWC	Cyber Crime Prevention against Women and Children
CCTNS	Crime and Criminal Tracking Network & Systems
CFSL	Central Forensic Science Laboratory
CGO	Central Government Offices
CIS	Cyber and Information Security
CP/ RGR	Child Pornography, Rape/Gang Rape
DFSS	Directorate of Forensic Science services
GOI	Government of India
IT ACT	Information Technology Act
MHA	Ministry of Home Affairs
MWCD	Ministry of Women & Child Development
NCFL	National Cyber Forensic Lab
NCRB	National Crime Records Bureau
NGO	Non-Governmental Organization
NH	National Highways
OM	Office Memorandum
PMU	Project Management Unit
R&D	Research and Development
SC	Supreme Court
UT	Union Territory
VC	Video Conferencing

EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

Introduction

The Ministry of Home Affairs had constituted an Expert Group vide OM No. 24013/102/Misc./2014-CSIR-III/14542-St dated 24th December 2014 to study the gaps and challenges and prepare a road map for effectively tackling cybercrimes in the country and give recommendations on all facets of cybercrime and to make recommendations on the way and means to cybercrime against women and children.

The Expert Group has identified the gaps and challenges in tackling cybercrime and made specific recommendations to combat cybercrime in the country. Based on these recommendations, the CCPWC Scheme was proposed with a total outlay of Rs. 195.83 Cr. Further, as in its order dated 23.10.2017 in the matter of Suo Motu Writ Petition no. 3/2015: "Prajwala (NGO) matter: Videos of Sexual Violence and Recommendations", the Hon'ble Supreme Court has issued directions to Government of India for creating a sub-project under CCPWC scheme. The sub-project was proposed with an outlay of Rs.27.368 Cr. The sub-project largely focuses on establishing mechanism to curtail the spread of obscene imagery online as well as to augment the online portal with a hotline to receive anonymous tips regarding CP/ RGR content/ cases.

Thus, the total outlay of "Cyber Crime Prevention against Women and Children (CCPWC) including sub-project" proposed at Rs. 223.198 Crores from Nirbhaya Funds of Ministry of Women & Child Development for the period 2017-2020. At present, the implementation period of Scheme was further extended for one year beyond 31.03.2020 i.e., up to 31.03.2021. Further, the proposal is under consideration for extending the implementation period of the scheme for 02 years beyond 31.03.2021.

The main objective of Cyber Crime Prevention against Women and Children (CCPWC) Scheme is to develop an effective mechanism to handle cybercrimes against women and children in the country. The scheme has a total estimated outlay of Rs. 223.198 Crores.

The main objectives of the scheme are as under:

1. To establish an online cybercrime reporting platform and associated monitoring units and hotline as proposed considering components of the sub-scheme. The total outlay will be Rs. Rs 36.648 Crores.
2. To establish an online monitoring facility for proactive identification, monitoring of CP/RGR content as well as analysis of complaints registered on the online reporting portal.
3. To establish a 24x7 hotline for accepting anonymous complaints of Child pornography, Rape/Gang rape imagery and to provide guidance to victims.
4. To establish a Hash Bank unit to facilitate removal of identified CP/RGR content in coordination with Content Hosting Providers (CSP's).
5. To establish one (1) National level advanced cyber forensic laboratory to be set up with the estimated cost of Rs.37.34 Crores.
6. To support 36 State/UTs with creation/upgrade of police training institutions/facility for cybercrime investigation training programs. The total outlay will be Rs. 95.76 Crores.
7. The total estimated cost for capacity building activity by using the above training facility will be Rs. 15.05 Crores. A total of 2500 Women Police Officers, 25000 Police Officers and 13000 Judicial Officers are proposed to be trained.
8. Rs. 15.72 Crore will be spent for citizen cybercrime awareness activities.
9. Rs. 15.00 Crores will be spent for R&D.
10. Rs.7.68 Crores will be spent towards on-boarding domain experts in the Project Management Unit.

Main Components of the CCPWC Scheme

1. Online Cybercrime Reporting Portal
2. National Cyber Forensic Lab
3. Capacity Building
4. Research and Development
5. Awareness Creation
6. Project Management Unit

Year of commencement: 2017-18

Financial Assistance under CCPWC Scheme: The scheme is wholly funded under Nirbhaya Funds of Ministry of Women & Child Development.

Methodology

The main aim of the study is to assess the effectiveness of the scheme and whether the scheme has been successful in achieving its objective of establishing effective infrastructure and mechanism to handle cybercrimes against women and children in the country.

The Study will focus on the following objectives:

1.1 Performance of the scheme based on the Output/Outcome indicators

1.2 Evaluation will be based on following parameters:

i. Implementation mechanism and progress,
ii. Achievement of deliverables,
iii. Need for extension of the implementation period and required time frame,
iv. Key Bottlenecks & Challenges.
v. Recommendations and suggestions.

I. Research Study Workflow

A. Research Objective:

To assess the effectiveness of the scheme and whether the scheme has been successful in achieving its objective of establishing effective infrastructure and mechanism to handle cybercrimes against women and children in the country.

To meet the above objective following steps of research process will be followed:

Step 1: Preliminary study:

- Review of Literatures and discussions with the CIS Division of MHA.
- Review of fund allocated under different subcomponents.

Step 2: Detailed discussions / Kickoff meeting

Step 3: Visits of offices and Data collection:

- Development of instruments for the study.
- Office Visit/ Discussion with officials concerned.

Step 4: Data Analysis and Report Writing

Data Collection and Analysis

The study team applied a mixed methodology approach and used a combination of quantitative and qualitative tools of data collection and analysis. The research study involved identification of the primary and secondary sources of information. Based on the kind of data available, instruments for the study were developed and data was collected.

The detailed research methodology and sampling design followed by the study team are as under: -

I. Collection of Secondary Data

The study team collected secondary information from the following sources: -

1) Official website of MHA
2) Copies of scheme related documents as provided by the MHA officials.
3) Scheme Guidelines, project status and updated notifications related to the scheme.

II. Collection of Primary Data

The study team collected primary information from the following sources: -

1) Interviews and discussions with the officials of CIS Division, MHA.
2) Online discussion meetings via video conferencing with the nodal officers of the main implementing agencies of the scheme, i.e., BPR&D, NCRB, DFSS and States/UTs.

Limitations of the Study

The following were a few of the limitations of this study:

1. Given, the study took place during the Covid-19 pandemic, lack of field visits attribute to one of the major the limitations of the study.
2. The meetings with State officials could not be arranged due to the limited availability of time and other restrictive factors.

Study Duration : 01 March 2021 – 31 March 2021

Salient Findings

1. As on 28.02.2021, under the CCPWC scheme, the total expenditure is Rs.11649.13 lakhs i.e., **52.20%** and the balance amount is Rs. 10670.67 lakhs i.e., **47.80%** of the total outlay. The total outlay under the scheme is Rs. 22319.8 lakhs.
2. Further, in 2017-18, the expenditure incurred was Rs. 8969.25 lakhs i.e., **76.99%** of the total expenditure; in 2018-19 it was Rs. 524.3 lakhs (**4.50%**); in 2019-20, the expenditure was Rs. 1768.48 lakhs (**15.18%**); and, in 2020-2021 till January 2021, the expenditure has been Rs. 387.1 lakhs (**3.32%**).
3. The component of online cybercrime reporting portal has been allocated a total of Rs. 3664.8 lakhs. However, the total expenditure incurred as on date has been Rs. 296.86 lakhs i.e., **8.10 %** of the total allocated amount.
4. The total expenditure incurred under NCFL(E) component is Rs. 553.42 lakhs i.e., **14.82 %** of the total allocated amount i.e., Rs. 3734 lakhs. The expenditure pertains to procurement of hardware/software tools, hiring of **37** technical professionals for the Lab and other operational expenditure.
5. The total allocation to States/UTs is Rs. 9577.23 lakhs and the total utilization is Rs. 3883.46 lakhs i.e., **40.54 %** of the total allocated amount. The total expenditure pertaining to the three subcomponents is Rs. 8456.50 lakhs (**88.3%**) for establishing Forensic Labs in each State/UT, Rs. 688.73 lakhs (**7.19%**) for conducting trainings, and Rs. 432 lakhs (**4.33%**) for hiring Jr. Cyber Consultant.
6. Under different categories of States/UTs, the total allocated amount to Category A is Rs. 3978.32 lakhs (**41.54%**), to Category B is Rs. 2637.25 lakhs (**27.54%**) and to Category C is Rs. 2961.65 lakhs i.e., **30.92%** of the total allocated amount. The total allocated amount is Rs. 9577.23 lakhs.
7. As on 28.02.2021, of the 36 States/UTs, 33 States/UTs received funding. Of the **33**, **14** States/UTs have utilized the funds for conducting trainings for LEAs.
8. The total number of Women police personnel trained is **1319** and the total number of Men police personnel trained is **10648**. The total number of Judicial officers trained is **762** while the total number of Public Prosecutors trained is **950**. The grand total number of personnel trained is **13679**.
9. As on 28.02.2021, the overall percentage of women police personnel trained under Capacity Building component of CCPWC comprised about **11%** of the total number of police personnel trained.

10. As on 28.02.2021, **19** States/UTs have utilized their funds for establishing Forensic lab-cum-training facilities but **17** States have established Labs-cum-training facilities.
11. As on 28.02.2021, a total of **12** States/UTs have utilized their funds for hiring Jr. Cyber Forensic Consultant while **14** States/UTs have hired the consultants.
12. A recurring expenditure of Rs. 172.66 lakhs (i.e., **11.51%** of the total allocated amount) have been incurred under the R&D component. And BPR&D, the implementing agency, has sanctioned a total of 9 projects. The total cost provision for this component under CCPWC is Rs. 1500 lakhs.
13. A total of Rs. 617.92 lakhs (i.e., **39.31%** of the total allocated amount) have been spent in spreading awareness against cybercrimes against women and children under Awareness Creation component. The total cost provision for this component under CCPWC is Rs. 1572 lakhs.
14. A total of Rs. 534.19 lakhs (i.e., **69.55 %** of the total allocated amount) have been spent on operationalizing the PMU component. The total cost provision for this component under CCPWC is Rs. 768 lakhs.

Suggestions and Recommendations

The suggestions and recommendations are as follows:

1. Emphasis on Fund Utilization

It is suggested that more focus be laid on the States/UTs still struggling with their fund utilization. Other States/UTs and stakeholders who have been able to utilise their funds may also continue to be encouraged and supported with sufficient fund allocation for the future activities.

2. Increase Manpower

It is emphasised to increase manpower enhanced by conducting trainings, be available in all States/UTs for handling cybercrimes against women and children.

3. Procurement of Advanced Tools and Technology

It is suggested that States/UTs which have been able to utilise funds in this direction may be encouraged and supported more for timely procurement of required equipment(s).

4. SOPs to be followed by all States/UTs LEAs

It is suggested that focus on development of standardised SOPs and their strict enforcement by all LEAs may be made an essential part of the scheme.

5. Development of a Mobile Application for Effective Reporting

Focus on developing a mobile application based on Android or iOS which is user-friendly and ensure user privacy. The App may also function as an Awareness creation tool by incorporating interactive infographics and videos for its end users.

6. Monitoring and Evaluation of Cybercrime Landscapes

A team of cyber experts may be present in all States/UTs as well as on a national level for ensuring proactive monitoring and evaluation of changing trends of cybercrimes. Regular meetings of these teams may take place for timely analysis of cybercrimes happening across the country.

7. Interactive Sessions with School and College Students

It is suggested that school and college level interactive sessions in the form of debate competitions, Hackathons, theatre activities and painting competitions etc. may be organized under the Awareness Creation component of CCPWC scheme.

8. Access to storage on Cloud space for quicker resolvement of cybercrime cases

Emphasis may be laid on procuring a virtual storage on cloud space and interlink it all the different portals.

9. Harnessing Predictive Analytics Technique in Cyber Security

It is emphasised to employ innovative and sophisticated techniques like predictive analytics in ensuring cyber security.

10. Integration of e-Court Services for Cybercrime Cases

It is, therefore, emphasised that CCPWC scheme may ensure faster integration of e-Court Services with the platform to aid in faster resolvement of the registered cybercrime cases.

11. Involvement of NGOs and Civil Society Groups in Cyber Safety Programmes

To strengthen the cyber ecosystem at large it is suggested to increase the involvement of NGOs and other Civil Society groups by organizing programmes on cyber awareness and security specific to women and children's issues.

12. Capacity Building and Awareness creation in Semi-urban and Rural Areas

To spread awareness among the semi-urban and rural area populations, broadcasting may be carried out in local dialects with the help of All India Radio (AIR) and Doordarshan channel (DD).

13. Engagement with national and international NGOs/ International bodies

Exchange program between private/ public bodies, NGOs and international bodies may be established for effective utilization of expertise and enhancement of capabilities. exchange

CHAPTER 1 : INTRODUCTION

1. INTRODUCTION

1.1. Background

The Ministry of Home Affairs had constituted an Expert Group vide OM No. 24013/102/Misc./2014-CSIR-III/14542-St dated 24th December 2014 to study the gaps and challenges and prepare a road map for effectively tackling cybercrimes in the country and give recommendations on all facets of cybercrime and to make recommendations on the way and means to cybercrime against women and children.

The Expert Group has identified the gaps and challenges in tackling cybercrime and made specific recommendations to combat cybercrime in the country. Based on these recommendations, the CCPWC Scheme was proposed with a total outlay of Rs. 195.83 Cr. Further, as in its order dated 23.10.2017 in the matter of Suo Motu Writ Petition no. 3/2015: "Prajwala (NGO) matter: Videos of Sexual Violence and Recommendations", the Hon'ble Supreme Court has issued directions to Government of India for creating a sub-project under CCPWC scheme. The sub-project was proposed with an outlay of Rs.27.368 Cr. The sub-project largely focuses on establishing mechanism to curtail the spread of obscene imagery online as well as to augment the online portal with a hotline to receive anonymous tips regarding CP/ RGR content/ cases.

Thus, the total outlay of "Cyber Crime Prevention against Women and Children (CCPWC) including sub-project" proposed at Rs. 223.198 Crores from Nirbhaya Funds of Ministry of Women & Child Development for the period 2017-2020. At present, the implementation period of Scheme was further extended for one year beyond 31.03.2020 i.e., up to 31.03.2021. Further, the proposal is under consideration for extending the implementation period of the scheme for 02 years beyond 31.03.2021.

According to India's Constitution, the Police and public order are State subjects, and the State is primarily responsible for the prevention, detection, and investigation of crime through their law enforcement machinery. The CCPWC scheme allows Law Enforcement Agencies (LEAs) to take legal action in line with the Indian Penal Code and the Information Technology to prevent cybercrimes against women and children.

1.2. Cyber Crime Prevention against Women and Children (CCPWC) Scheme

The main objective of Cyber Crime Prevention against Women and Children (CCPWC) Scheme is to develop an effective mechanism to handle cybercrimes against women and children in the country. The scheme has a total estimated outlay of Rs. 223.198 Crores and main objectives of the scheme are as under:

1. To establish an online cybercrime reporting platform and associated monitoring units and hotline as proposed considering components of the sub-scheme. The total outlay will be Rs. 36.648 Crores.
2. Establish an online monitoring facility for proactive identification, monitoring of CP/RGR content as well as analysis of complaints registered on the online reporting portal.
3. Establish a 24x7 hotline for accepting anonymous complaints of Child pornography, Rape/Gang rape imagery and to provide guidance to victims.
4. Establish a Hash Bank unit to facilitate removal of identified CP/RGR content in coordination with Content Hosting Providers (CSP's).
5. Establish one (1) National level advanced cyber forensic laboratory to be set up with the estimated cost of Rs.37.34 Crores.
6. Support 36 State/UTs with creation/upgrade of police training institutions/facility for cybercrime investigation training programs. The total outlay will be Rs. 95.76 Crores.
7. The total estimated cost for capacity building activity by using the above training facility will be Rs. 15.05 Crores. A total of 2500 Women Police Officers, 25000 Police Officers and 13000 Judicial Officers are proposed to be trained.
8. Rs. 15.72 Crore will be spent for citizen cybercrime awareness activities.
9. Rs. 15.00 Crores will be spent for R&D.
10. Rs.7.68 Crores will be spent towards on-boarding domain experts in the Project Management Unit.

Main Components of the CCPWC Scheme

1. Online Cybercrime Reporting Portal
2. National Cyber Forensic Lab
3. Capacity Building
4. Research and Development
5. Awareness Creation
6. Project Management Unit

Year of commencement: 2017-18

Financial Assistance under CCPWC Scheme

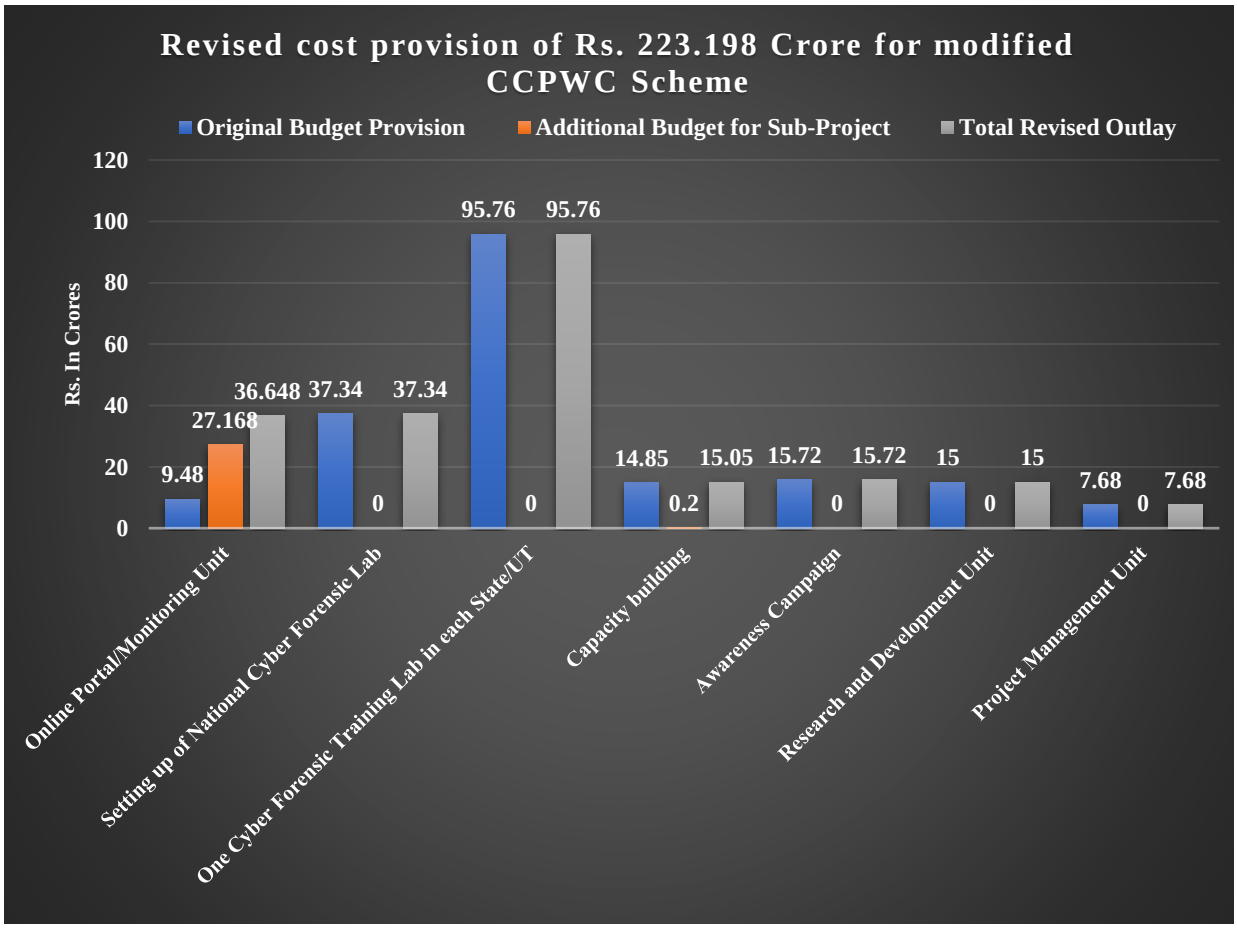
The scheme is wholly funded under Nirbhaya Funds of Ministry of Women & Child Development.

At present, the CCPWC Scheme has been sanctioned for Rs.223.198 Crore including Recurring & Non-recurring cost provisions. The below tables show the break-up of the revised cost provision of Rs. 223.198 Crore for modified CCPWC Scheme:

Table 1 Break-up of the revised cost provision of Rs. 223.198 Crore for modified CCPWC Scheme

Component	Original Budget Provision	Additional Budget for Sub-Project	Total Revised Outlay
Total (Rs. In Crores)	195.83	27.368	223.198

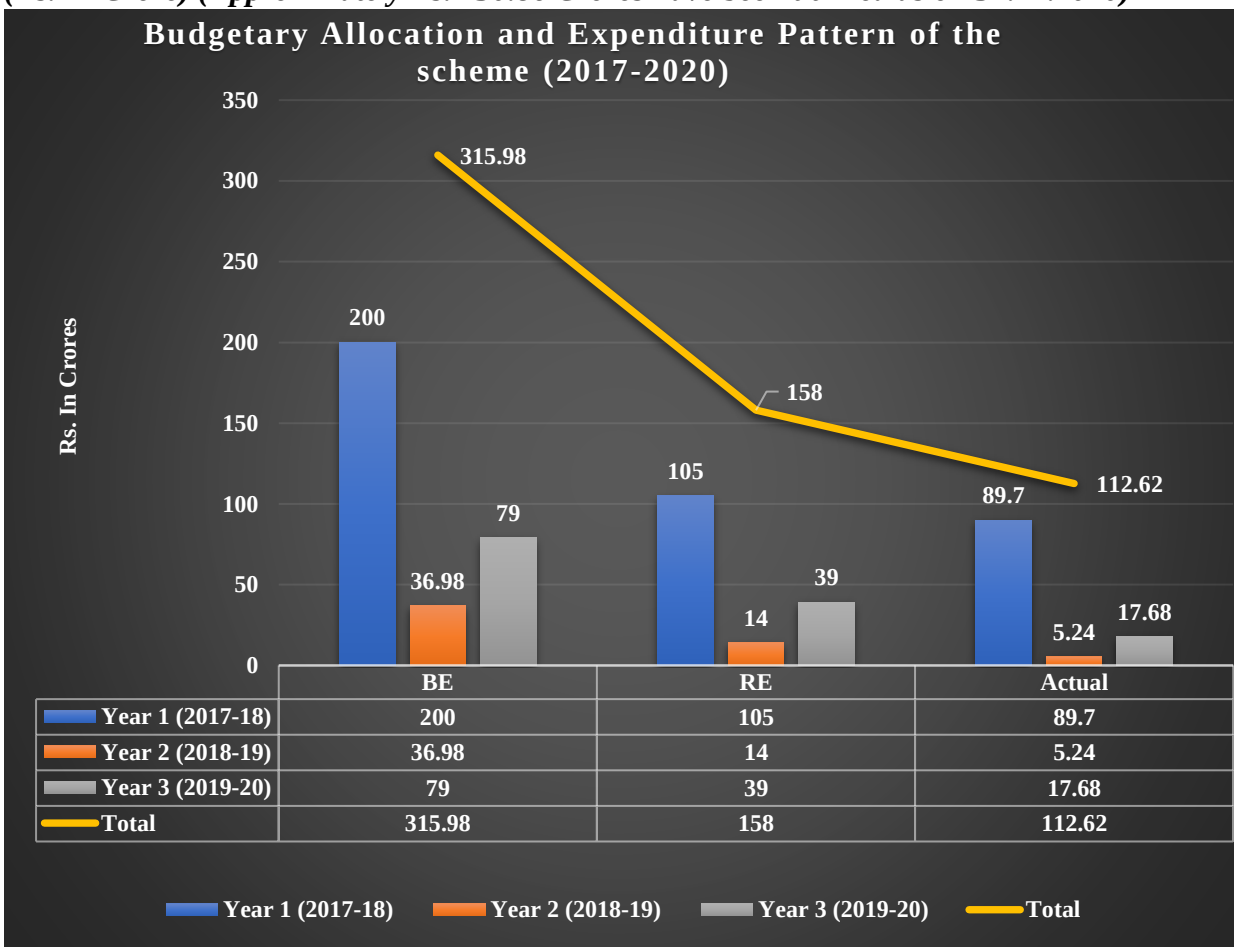
Break-up of the total outlay under is different components of the scheme



Graph 1 Revised cost provision of Rs. 223.198 Crore for modified CCPWC Scheme

Budgetary allocation and expenditure pattern of the scheme

(Rs. In Crore) (Approximately Rs. 130.86 Crores have been utilized as on 31.12.2020)



Graph 2 Budgetary allocation and expenditure pattern of the scheme (2017-2020)

Implementation Mechanism of the Scheme

CCPWC Scheme is a central sector scheme. CCPWC is to function as the coordinating body at national level to tackle all forms of cyber-crime against women and children. The scheme has been in implementation since 2017 and has been further extended for one year beyond 31.03.2020 i.e., up to 31.03.2021. The proposal to further extend the implementation period of Scheme for two years beyond 31.03.2021 is under process.

CIS Division of MHA examines and processes the implementation plan and funding requirement initiated by the implementing agencies/stakeholders and allocates budget after following codal formalities. Output/Outcome of each component is examined based on

physical deliverables/statistics wherever possible and through questionnaire/interview in other cases.

Under the component 'Capacity Building' funds are placed with States/UTs for its implementation. For implementation of components under the scheme, funds placed with various stakeholders are given below:

Table 2 Scheme Components and Stakeholders

S. No.	Scheme Component	Implementing Agency
1	Capacity Building	All States/UT's
2	Setting up of a State-of-the-Art Forensic Laboratory at CFSL, Hyderabad	DFSS, CGO Complex, New Delhi
3	Development and Maintenance of Online Cybercrime Reporting Portal/Pro-active monitoring	NCRB, Mahipalpur, NH-8, New Delhi
4	Research & Development	BPR&D, NH-8, Mahipalpur, New Delhi

Sub-Project under Cyber Crime Prevention against Women and Children Scheme

In its order dated 23.10.2017 in the matter of Suo Motu Writ Petition no. 3/2015: "Prajwal (NGO) matter: Videos of Sexual Violence and Recommendations", the Hon'ble Supreme Court has issued directions to Government of India for creating a sub-project under CCPWC scheme. The sub-project was proposed with an outlay of Rs.27.368 Cr. The sub-project largely focuses on establishing mechanism to curtail the spread of obscene imagery online as well as to augment the online portal with a hotline to receive anonymous tips regarding CP/ RGR content/ cases.

Objective of the subproject under CCPWC scheme

The proposed sub-project under the CCPWC scheme in compliance to the directions of Hon'ble Supreme Court's order dated 23-10-2017, aims to achieve following objectives:

1. Online reporting of cybercrime
2. Availability of adequate tools and technology
3. Proactive monitoring to curtail obscene content.
4. Engagement with national and international NGOs/ International bodies

The below tables show the break-up of expenses (Non-recurring & Recurring) for the sub-project under CCPWC scheme as represented below (Rs. in Lakh):

Table 3 Break-up of expenses (Non-recurring & Recurring) for the sub-project under CCPWC scheme

S. No.	**Head**	**Proposed cost of Sub-project CCPWC scheme**
1	Non-recurring	1105
2	Recurring	1631.8
Total		2736.8

The below tables show the break-up of expenses (component-wise) for sub-project under CCPWC scheme(Rs. in Lakh):

Table 4 Break-up of expenses (component-wise) for sub-project

S. No.	**Head**	**Cost of sub-project under CCPWC scheme**		
		2 Years Non-Recurring cost	**2 Years Recurring cost**	**Total Cost**
1	Obscene Content Reporting Portal and Helpline	470	65	535
2	Obscene Content Analysis and Coordination Unit	20	1360.8	1380.8
	(a)Hash Bank	19	34	53
	(b)Proactive monitoring	550	120	670
	(c)Coordination with entities	46	32	78
3	Capacity Building		20	20
Total(Rs. in Lakh)		1105	1631.8	2736.8

Table 5 Details of Manpower requirement under subproject of CCPWC

S. No.	**Unit**	**Persons hired from Industry**
1	Obscene content analysis and coordination	22
	Total	**22**

The scheme and the sub-project are analysed in detail in Chapter 2 and Chapter 3.

1.3. Objective of the Study

The main aim of the study is to assess the effectiveness of the scheme and whether the scheme has been successful in achieving its objective of establishing effective infrastructure and mechanism to handle cybercrimes against women and children in the country.

The Study will focus on the following objectives:

1.1 Performance of the scheme based on the Output/Outcome indicators

1.2 Evaluation will be based on following parameters:

i. Implementation mechanism and progress,

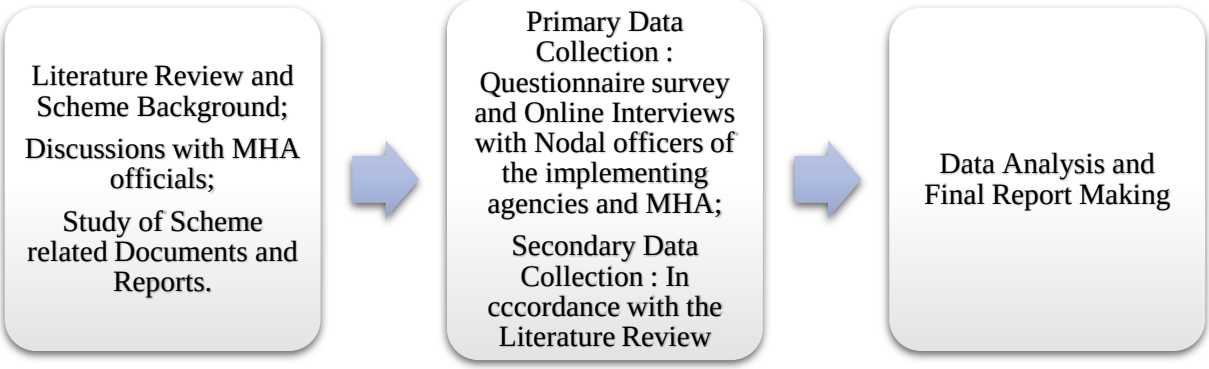
ii. Achievement of deliverables,

iii. Need for extension of the implementation period and required time frame,

iv. Key Bottlenecks & Challenges.

v. Recommendations and suggestions.

I. Research Study Workflow



A. Research Objective:

To assess the effectiveness of the scheme and whether the scheme has been successful in achieving its objective of establishing effective infrastructure and mechanism to handle cybercrimes against women and children in the country.

To meet the above objective following steps of research process will be followed:

Step 1: Preliminary study:

- Review of Literatures and discussions with the CIS Division of MHA.
- Review of fund allocated under different components.

Step 2: Detailed discussions / Kickoff meeting

Step 3: Visits of offices and Data collection:

- Development of instruments for the study.
- Office Visit/ Discussion with officials concerned.

Step 4: Data Analysis and Report Writing

B. Data Collection Methodology:

1. Primary data collection: Questionnaire and interview schedule
2. Secondary Data collection: Literature review of scheme related documents.

II. Methodology

The study team applied a mixed methodology approach and used a combination of quantitative and qualitative tools of data collection and analysis. The research study involved identification of the primary and secondary sources of information. Based on the kind of data available, instruments for the study were developed and data was collected.

The detailed research methodology and sampling design followed by the study team are as under: -

A. **Identification of the Scheme:** Scheme Guidelines and other relevant documents provided by the CIS Division of MHA were analysed and parameters were formulated. Based on the parameters the agenda points and questionnaires were prepared and data was collected.

B. **Designing of instruments for the study:** Following parameters were taken into consideration for the evaluation study. Based on these agenda points and questionnaires were prepared.

1) Implementation mechanism and progress,
2) Achievement of deliverables,
3) Need for extension of the implementation period and required time frame,
4) Key Bottlenecks & Challenges.
5) Recommendations and suggestions.

C. **Data Collection :**

The data collection began with the Kickoff meeting and subsequent meetings with the CIS Division officials at the Ministry of Home Affairs. The data pertaining to scheme's sub-project and components was collected through questionnaire and online VC meetings with the stakeholders.

I. Collection of Secondary Data

The study team collected secondary information from the following sources: -

1) Official website of MHA
2) Copies of scheme related documents as provided by the MHA officials.
3) Scheme Guidelines, project status and updated notifications related to the scheme.

II. Collection of Primary Data

The study team collected primary information from the following sources: -

1) Interviews and discussions with the officials of CIS Division, MHA.
2) Online discussion meetings via video conferencing with the nodal officers of the main implementing agencies of the scheme, i.e., BPR&D, NCRB, DFSS and States/UTs.

The Questionnaires pertaining to the evaluation studies are annexed at Annexure I, II &III.

1.4. Limitations of the Study

The following were a few of the limitations of this study:

1. Given, the study took place during the Covid-19 pandemic, lack of field visits attribute to one of the major the limitations of the study.
2. The meetings with State officials could not be arranged due to the limited availability of time and other restrictive factors.

Study Duration : 01 March 2021 – 31 March 2021

CHAPTER 2 :

COMPONENTS OF CCPWC

2. COMPONENTS OF CCPWC

2.1. Online Cybercrime Reporting Portal

As part of Cyber Crime Prevention for Women and Children (CCPWC) scheme a "Cybercrime Reporting Portal (https://cybercrime.gov.in) has been launched on 20 September 2018. National Crime Records Bureau has been designated as Nodal Agency for operating & maintenance of Cybercrime Reporting Portal.

The online cybercrime reporting portal caters to complaints pertaining to online Child Pornography (CP) / Child Sexual Abuse Material (CSAM) or sexually explicit content such as Rape / Gang Rape (CP / RGR) content. The portal is designed in a user-friendly way and aims to enable complainants to report cases without disclosing their identity. This facility will not only assist victims / complainants but help civil society organizations and citizens to anonymously report complaints pertaining to CP, CSAM or sexually explicit content such as Rape/Gang Rape. The complainants can also upload the objectionable content and URL to assist in the investigations by the State Police. The complaints registered on this portal are handled by the police authorities of respective States and Union Territories.

Figure 1 Launch of the Online reporting portal on 20th September 2018 (Source : PIB)

The Hon'ble Union Home Minister, Shri Rajnath Singh launched the cybercrime reporting portal in New Delhi on September 20, 2018. The Hon'ble Union Minister for Women and Child Development, Smt. Maneka Sanjay Gandhi, the Hon'ble Ministers of State for Home Affairs, Shri Kiren Rijiju and Shri Hansraj Gangaram Ahir and the Union Home Secretary, Shri Rajiv Gauba were also present.

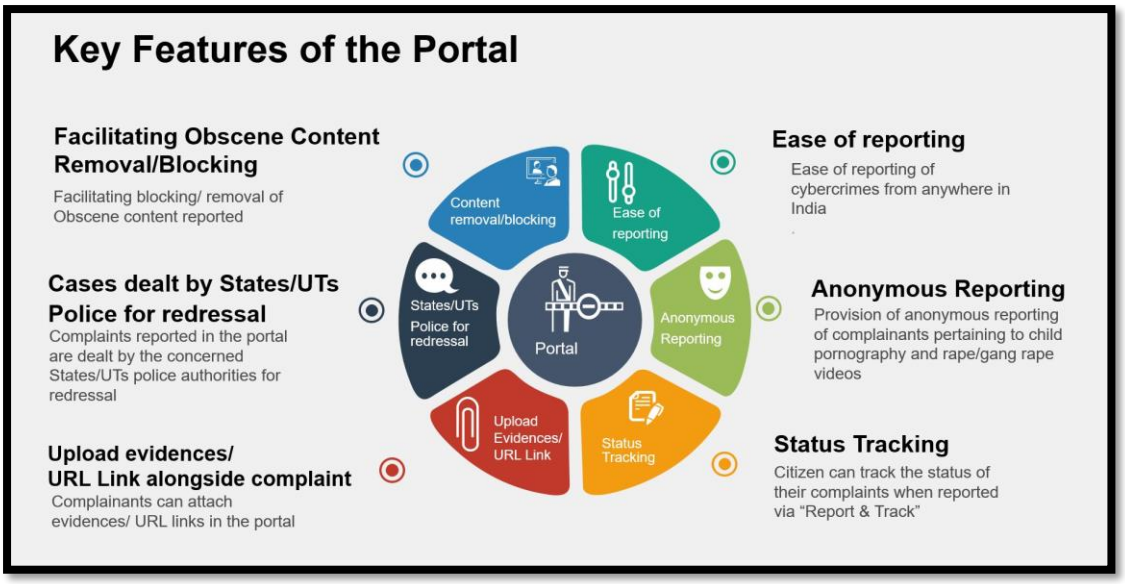


Figure 2 Key Features of the Online National Cybercrime Reporting Portal (Source : SheRAKSHA, MHA)

Figure 3 Snapshot of the Homepage of the Online portal

Role of the Portal in helping the LEAs: Complaints reported by citizen through Cybercrime reporting portal are attended by the LEAs of respective State Police to access and take required actions on. Police officials handling cybercrimes against women & children further ensures that the timely action is being taken on these complaints.

Moreover, the Cyber Tipline Reports shared by National Centre for Missing and Exploited Children (NCMEC), USA with NCRB are shared with States/UTs through the portal/CDs.

Categories of cybercrime against women and children addressed on the portal are:

1. Child Pornography (CP)-Child Sexual Abuse Material (CSAM)
2. Rape/Gang Rape(RGR)-Sexually Abusive Content
3. Publishing or Transmitting Sexually Obscene material in electronic form.
4. Publishing or transmitting material containing sexually explicit act in electronic form.

Present Status with coverage of scheme (operational/non-operational):

S. No.	Name of Component	Status	Remarks
1.	Online Cybercrime Reporting Portal	Operational	The cybercrime reporting portal was launched on 20.09.2018 which allowed citizens to report online content pertaining to Child Pornography/CSAM or sexually explicit content such as Rape/Gang Rape (CP/RGR) and revamped version of the portal was launched on 30.8.2019 to enable citizens to report complaints of all types of cybercrime with special focus on cybercrimes against women and children. Central Helpline number **155260** is also made available to citizens for any assistance required related to the portal.

2.2. National Cyber Forensic Laboratory, NCFL (E)

Under the CCPWC Scheme, a State-of-the-Art Forensic Laboratory has been set up at CFSL, Hyderabad through, DFSS, New Delhi to facilitate the investigation, analysis and reporting the cybercrime incident against women and children in a possible less turnaround time.
Establishment of the lab officially referred to as, NCFL (E), aims to provide necessary forensic support in cases of evidence related to cybercrime, preserving the evidence and its analysis in line with the provisions of IT Act and Evidence Act and will reduce turnaround time.

Figure 4 CFSL, Hyderabad (Source: DFSS Website)

Details of activities undertaken in setting up of NCFL(E) are as follows:

a) Procurement of Hardware/Software Tools.
b) Hiring of 37 technical professions
c) Other operational expenditure

Present Status with coverage of scheme (operational/non-operational):

S. No.	Name of Component	Status	Remarks
1.	National Cyber Forensic Lab	Under Establishment	It is Partially operational. Most of the hardware & software has been procured and installed. The proposed Lab is likely to be made fully operational in the current financial year. 37 technical professionals have been hired.

2.3. Capacity Building

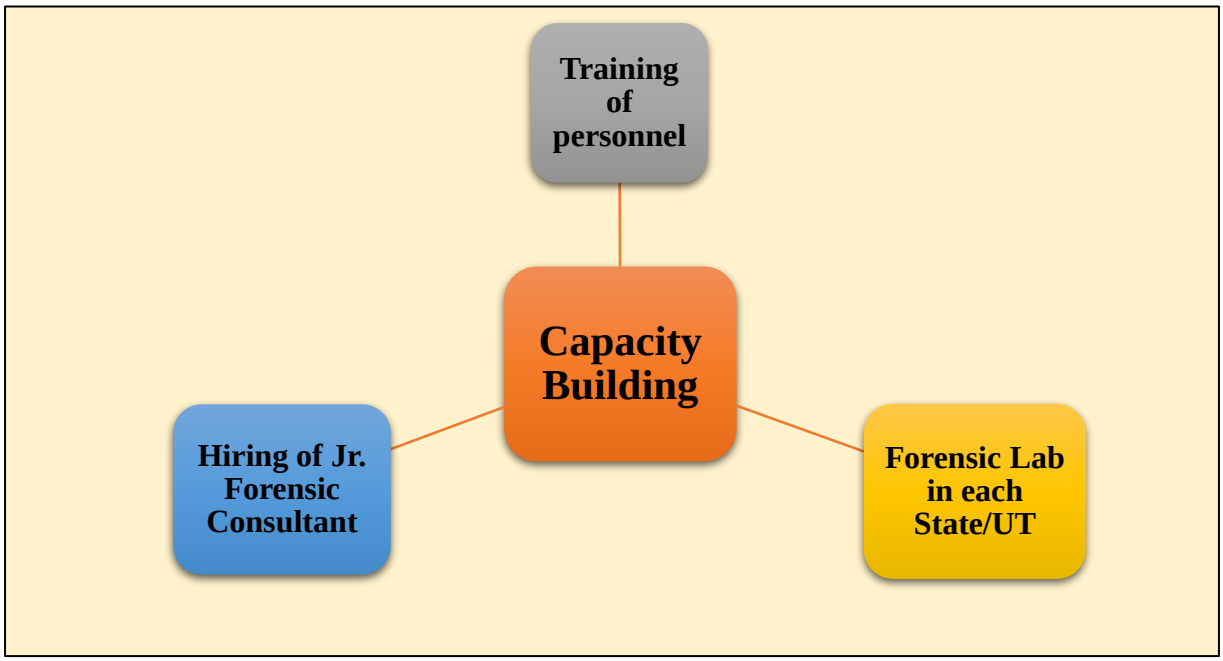


Figure 5 Different components of Capacity Building under CCPWC

This component entails strengthening the knowledge and skills of key stakeholders so that they have better understanding of all facets of cybercrime investigation, digital forensic, evidence collection etc., in-general, and particularly cybercrime against women and children.

As part of CCPWC scheme, a total of 2500 Women Police Officers, 25000 Police Officers and 13000 Judicial Officers have been proposed to be trained under the Capacity Building component. Funds have been released to all the States/UTs for its implementation. In this regard, cybercrime focused training programs have been developed in various format like short term courses, long term courses for police, prosecutors, judicial officers and other law enforcement and investigation agencies in the state and centre.

In addition to this, Forensic labs-cum-training facilities are to be established in each State and UT across the country under the same component. All states/UTs are required to setup cyber forensic training facility as per indicative configuration given below:

Grant released to State/UT	**Rs. 3.94 Crore**	**Rs. 2.30 Crore**	**Rs. 1.48 Crore**
Recommended Workstations in Lab	25 or more as per need of the State Govt.	25	15

In addition to recommended number of PC workstations, one laptop is to be purchased for the training lab. All workstations need to be networked and provided internet facility. Wi-Fi facility may also be provided in the lab for training purpose.

Selection of appropriate tools for training lab may be made by respective States/UT taking note of the training tools. Hardware already available at the training location where such lab is being setup. States/UTs may choose any other useful tool also if felt necessary, for capacity building purpose. Basic cyber forensic tools to be purchased in such a number so as to ensure that each trainee gets individual kit for hands on exposure.

An indicative list of tools as prescribed under the scheme is given below:

Table 6 List of Tools prescribed under CCPWC

Basic Cyber Forensic Tools	
S. No.	**Tool**
1	CDR analysis
2	Disk Forensics
3	Mobile Forensics Kit
4	Write Blockers (SATA/IDE)
5	Pen Drives
6	Card readers
7	Smart phones
8	Hard disk (capacity min 40 GB max 80/160 GB)
9	Social media analysis/OSINT Tools
Other Cyber Forensic Tools	
S. No.	**Tool**
10	Disk Imaging
11	Live forensics
12	Steganography detection Tool
13	Network forensics
14	GPS forensics
15	Memory forensics
16	Web Browser analysis tools
17	Registry Forensics

18	Password Recovery Tools
19	Audio/video Forensics and CCTV analysis
20	Case management software
21	Data recovery from damaged hard disk
22	Drive Wiper
23	Remote system forensic
24	Malware Analyzer

Present Status with coverage of scheme (operational/non-operational):

S. No.	Name of Component	Status	Remarks
1.	Capacity Building	Underway	One Cyber Forensic-cum-Training Laboratory in each State/UT is to be established. It has been commenced in 17 States/UTs. Remaining States/UTs are at either completion or tendering stage. 40500 LEAs/Judicial Officers/Prosecutors are to be trained by States/UTs. So far more than 13500 police personnel/public prosecutors/judicial officers have been trained and remaining officials are being trained.

2.4. Awareness Creation

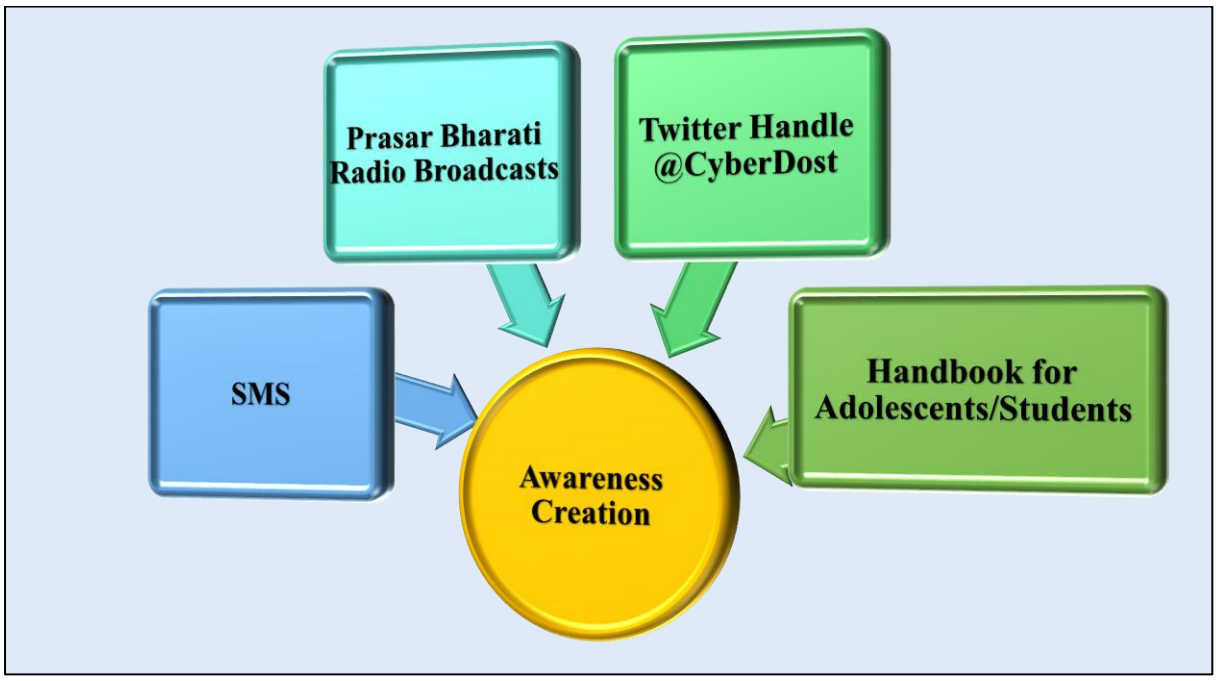


Figure 6 Different mediums of Awareness creation under CCPWC

This unit aims to operationalise a well-defined awareness campaign to educate the people about cyber-crimes and protect them from being victim of a cybercrime. Under CCPWC scheme, an awareness campaign has been planned to reach out to masses and reinforce messages on prevention cybercrimes against women and children.

About @CyberDost

Cyber Dost is a Twitter handle, @CyberDost, floated by the Ministry of Home Affairs back in March 2018 that advises people on how to keep their personal and financial details safe while using them online. The account, marked as a cyber-safety and cybersecurity awareness handle, has close to 299.6K followers with 754 tweets posted so far (as on 21.03.2021).

The handle covers topics ranging from safe online banking to identity theft and even measures to ensure safe internet usage for children. The Cyber Dost handle also directs victims of cybercrimes towards the correct channels to file their complaints. People can post their queries on its feed and get an answer about a suitable course of action. The handle also posts tips for public and government officials to keep them updated on the best practices regarding

cybersecurity. The handle also tries to generate awareness to check the spread of fake news, which has been making headlines for some time now.

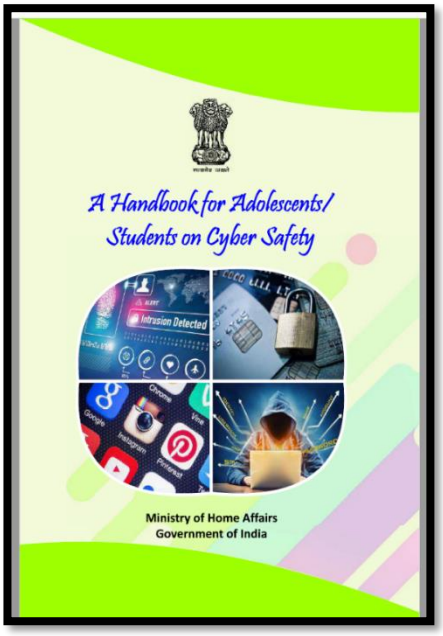


Figure 7 Cover page of the Handbook published by MHA

Figure 8 Snapshot of Twitter Handle of @CyberDost

Present Status with coverage of scheme (operational/non-operational):

S. No.	Name of Component	Status	Remarks
1.	Awareness Creation	Undertaken	MHA launched Radio campaign across the country for six months to spread awareness against cybercrimes. MHA has launched Twitter Handle @CyberDost for dissemination of messages on cybercrime. Published "Handbook for Adolescents/Students."

2.5. Research and Development

In order to develop effective tools to detect obscene and objectionable content in the cyberspace and to continuously refine such tools, BPR&D, MHA, New Delhi has been authorized to take up research and development activities in partnership with research and academic institutions across the country.

Present Status with coverage of scheme (operational/non-operational):

S. No.	Name of Component	Status	Remarks
1.	Research and Development	Underway	BPR&D has been designated as Nodal agency for supervision and monitoring of R&D projects. 9 R&D projects have been identified approved for its execution in the cybercrimes. Funds have been released to the selected institutions as per conditions laid down in MoU signed between BPR&D and the Institutes concerned.

List of Projects under CCPWC and respective Institutions

Table 7 List of Projects under CCPWC and respective Institutions

S.No.	Project Title	Institute Name
1.	A web browser based intelligent kernel tool for automatic detection and blocking of obscene image and video contents in real time	IIIT Allahabad
2.	Proactive Monitoring of Online Social Network for Prevention of Crime against Women & Children (PMOPCWC)	NIT Calicut
3.	Detection and Prevention of Forged Obscene Images/Videos in the Social Networks using Machine Learning (A Social Media Engine for Discovering Doctoring in Obscene Multimedia)	IIT Jodhpur

4.	Detection and Prevention of Forged Obscene Images/Videos in the Social Networks using Machine Learning	IIIT DM Kancheepuram
5.	Design of and Development of Intelligent Algorithms for Analysis and Detection of Obscene Content and Forgery in the Images Available in Social Media Platform	NIT Meghalaya
6.	Centre of Excellence in Cyber Crime Prevention against Women and Children -Al-based Tools for Women and Children Safety	IIT Patna
7.	THE SENTNEL – Active Intelligent Agent for Actionable Intelligence on Cybercrime Control and Prevention	IIT Goa
8.	Mobilizing India to curb online child/ women sex abuse using indigenous Technologies	Punjab Engineering college, Chandigarh
9.	Establishment of Centre of Excellence for Cybercrime Prevention against Women & Children	Veermata Jijabai Technological Institute (VJTI), Mumbai

2.6. Project Management Unit

The PMU is a dedicated professional project management unit to ensure that all the initiatives under this scheme are properly monitored and implemented. This unit will assist MHA in monitoring the project implementation.

Present Status with coverage of scheme (operational/non-operational):

S. No.	Name of Component	Status	Remarks
1.	Project Management Unit	Established	PMU has been set up in 2018 and function up to March 2020. Keeping in view the proposed extension of the CCPWC beyond 31.03.2021, services of PMU is required in assisting the Ministry for monitoring and implementations of all the initiatives under the scheme.

2.7. Sub-project under CCPWC

The proposed sub-project under the CCPWC scheme in compliance with the directions of Hon'ble Supreme Court's order dated 23-10-2017, aims to achieve following objectives:

1. **Online reporting of cybercrime:** This aims to enable reporting of obscene content anonymously as well as by furnishing details of complainant. States/UTs have been extended access to this portal for viewing and acting upon the complaints pertaining to their jurisdiction. While the current portal enables the victim/ complainant to lodge grievances it does not offer any feature for law enforcement agencies to avoid duplication in effort if the same content is reported from another state/ UT. In addition to this, considering the various multimedia formats and sensitivity associated with the content reported it is required to restrict download of content to systems across various state/ UT cyber cells. Further, the portal also requires a capability to ingest feeds from multiple sources. Hence, a comprehensive case management solution is necessary to help facilitate various state/UTs to manage cases allocated to them, issue notice to and seek compliance from CHPs within the same workflow and to flag content for Hash generation. Considering the above, both the citizen facing, and police portal will require re-development.

2. **Availability of adequate Tools and Technology:** Landscape of the cyber world is fast changing by Internet of Things (connected devices), Internet of People (social networking sites), Internet of Commerce (online shopping sites), and new generation intelligent network of telecommunication leading to different possibilities of cybercrime against women and children, which is now only restricted to computers and its networks, but has also extended to almost every electronic device and cyber criminals are using advanced cyber weapons to commit crime against women and children. Therefore, advanced tools are required for monitoring and prevention of cybercrime as well as monitoring criminal activities against women and children on social media.

3. **Proactive monitoring to curtail obscene content:** This aims to reduce the crime against children and women especially online sexual abuse, and pornographic content circulated on social media and made accessible over other content hosting platforms needs to be closely monitored for strict compliance to national laws.

4. **Engagement with national and international NGOs/ International bodies:** This aims to engage NGOs, international bodies, and industries for effective tackling of cybercrime and exchange of expertise. People's exchange program between private/ public bodies, NGOs and international bodies must be established for effective utilization of expertise and enhancement of capabilities.

Year- wise outputs/ deliverables of the sub-project under CCPWC

Table 8 Year- wise outputs/ deliverables of the sub-project under CCPWC

Unit	Focus area/ Output
Online reporting portal	Provide advanced analytics and case management to LEAs for better handling of complaints filed on the portal and direct capturing of tips received from NCMEC, USA and other such international agencies.
Helpline	Receive telephonic tip-off complaints related to CP/ RGR content.
Obscene Content Monitoring	• Use advanced tools to scan content on the internet including dark web and deep web with special focus on identifying CP and RGR content. • Use advanced tools to scan content over social media and other public/ open channels such as blogs, news boards etc. which publish, re-direct to CP/ RGR content.
Hash bank	• Generate hash for images received on the online portal and populate hash bank. • Receive Hash values from international partner's and analyse content over the internet. • Liaise with content hosting providers to ensure content matching Hash submitted is removed/ taken down. • Maintain a keyword bank by tracking popular search keywords linked with CP/ RGR content as well as other obscene content.

Obscene Content Monitoring: This unit aims to use sophisticated technologies such as crawlers to identify obscene content and generated leads which will be handed over to Complaint analysis & coordination Unit for further action. The Obscene Content Monitoring Unit shall be manned by a team of 22 professionals. This unit will also develop all the required

SOPs and workflows for technical investigation of the reported cyber-crime cases by the central and state / UT agencies. This unit will do the following:

- Provide a user-friendly interface over online for reporting a cyber incident.
- Coordinating with the local law enforcement agencies in passing on the registered complaints.
- Acting as a nodal agency in coordinating with the local law enforcement agencies and the services provider by providing a channel for sharing the evidential information.
- Preliminary analysis of each reported crime.
- Defining resolution processes for various categories of cyber-crimes.
- Taking appropriate actions as per the defined processes for resolution of the complaints.
- Publish annual analytical reports on online cyber-crime reported.
- Work closely with forensic and monitoring/ vigilance.

Hash bank: The MHA also aims to establish a Hash bank which will manage a central repository of hash for reference to law enforcement and regulatory agencies at the national, state, and local level for cyber-crime related information. This unit will generate hash of each complaint validated by State / UT police and update the hash bank.

Manpower required under sub-project of CCPWC

22 skilled technical manpower including consultants will be hired through outsourcing as per the various provision of GFR. Their responsibility will include the following activities:

1. Use sophisticated technologies such as crawlers to identify obscene content and analyse generated leads for further activity such as for building information regarding potential forums, links where CP/ RGR content is hosted, published, or distributed etc.
2. Validation (as needed) of reported obscene content by international agencies which involves (1)Forwarding content blocking request for validated obscene content, and (2) Forwarding complaints to concerned law enforcement agencies for appropriate action as per the defined processes.
3. Generate Hash for CP/RGR content
4. Coordinate with other entities such as NCMEC, INHOPE etc.
5. Coordinate with Content Hosting Providers (CHP's)
6. Contribute to keyword bank and Hash bank.

Present Status with coverage of scheme (operational/non-operational):

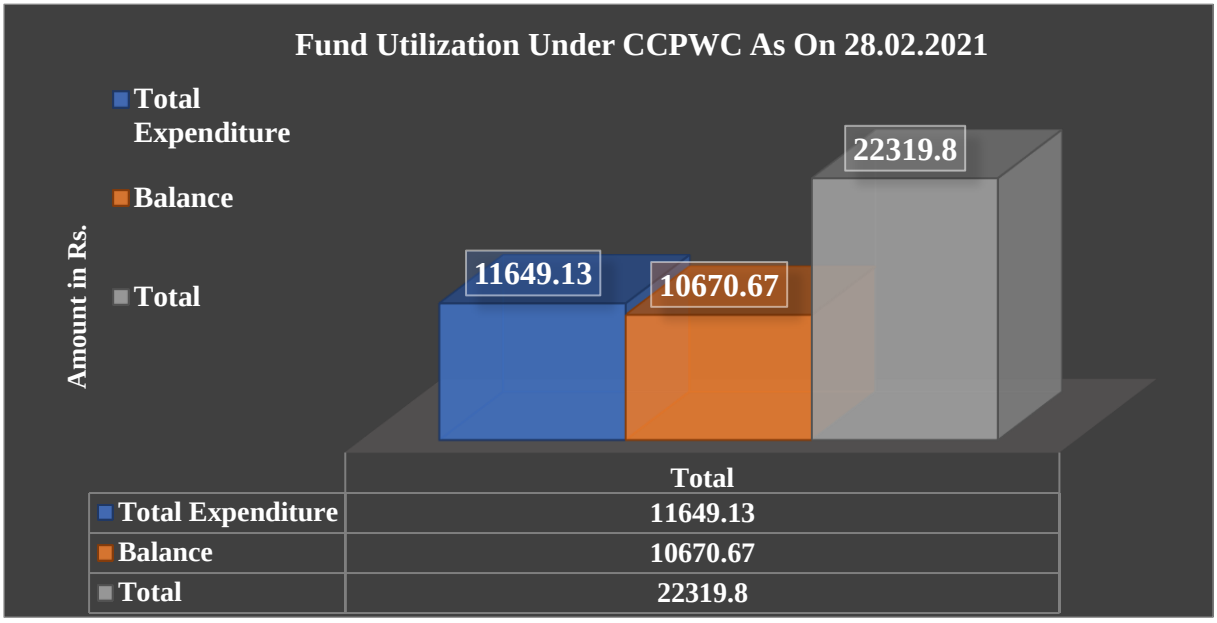
S. No.	Name of Component	Status	Remarks
1.	Monitoring Unit	Under Establishment	For setting up of pro-active monitoring unit for CSAM & RGR contents in web space by NCRB in consultation with C-DAC Mumbai is presently under consideration of the Ministry for its execution.

CHAPTER 3 :

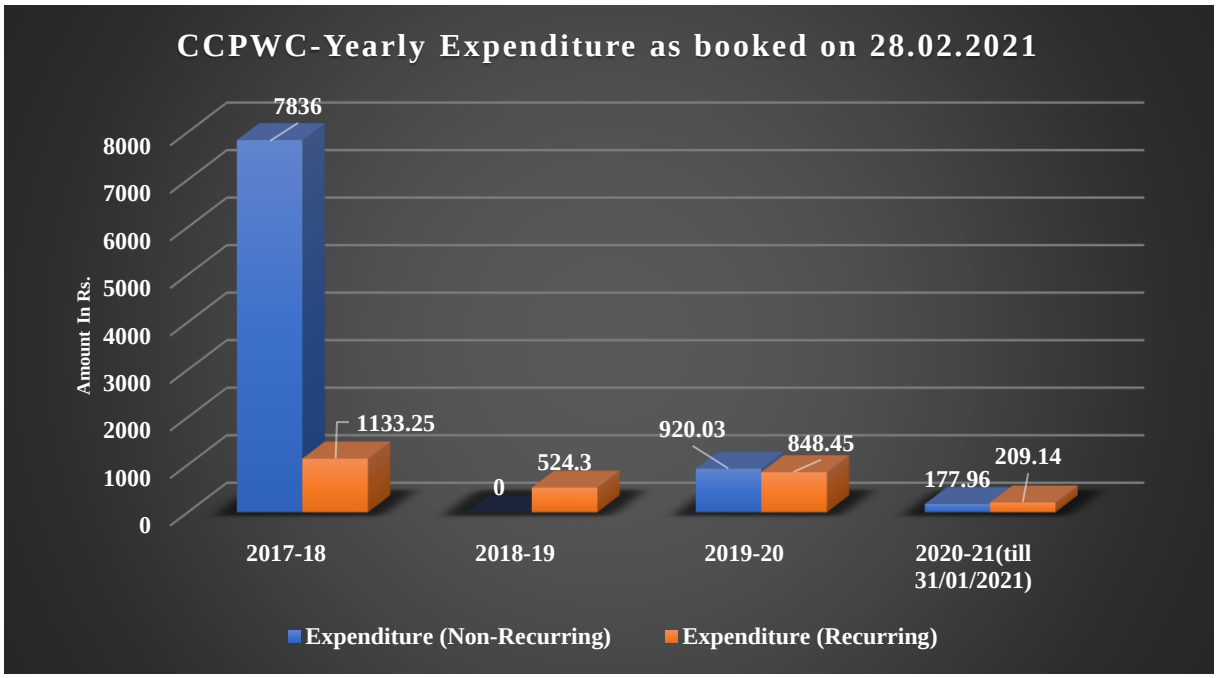
DATA ANALYSIS AND FINDINGS

3. DATA ANALYSIS AND FINDINGS

3.1. Overall Fund Distribution and Utilization under the CCPWC Scheme



Graph 4 Fund Utilization Under CCPWC as on 28.02.2021

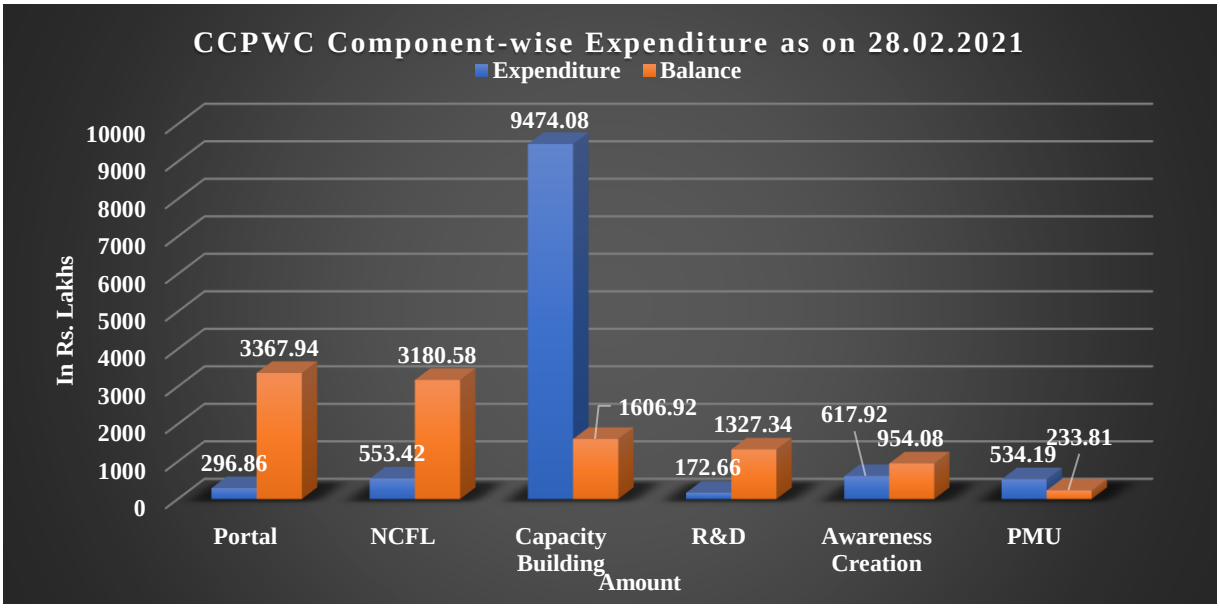


Graph 3 CCPWC-Yearly Expenditure as booked on 28.02.2021.

Year	2017-18	2018-19	2019-20	2020-21(till 28/02/2021)	Grand Total (Rs. In lakh)
Expenditure	8969.25	524.3	1768.48	387.1	11649.13

Graph 4 and above table represent the overall fund allocation and utilization under CCPWC Scheme as booked on 28 February 2021. As on 28.02.2021, under the CCPWC scheme, the total expenditure is Rs.11649.13 lakhs i.e., approximately **52.20%** of the total allocated amount and the balance amount is Rs. 10670.67 lakhs (i.e., **47.80%**). The total outlay under the scheme is Rs. 22319.8 lakhs.

Graph 3 depicts the year-wise total expenditure under the scheme since its inception in 2017 to 28 February 2021. In 2017-18, the expenditure was Rs. 8969.25 lakhs i.e., **76.99%** of the total expenditure; in 2018-19 it was Rs. 524.3 lakhs i.e., **4.50%** of the total expenditure ; in 2019-20, the expenditure was Rs. 1768.48 lakhs i.e., **15.18%** of the total expenditure; and, in 2020-2021 till February 2021, the expenditure is Rs. 387.1 lakhs i.e., **3.32%** of the total expenditure. All the amounts total to the tune of Rs. 11649.13 lakhs which is exactly the total expenditure as depicted in Graph 1.

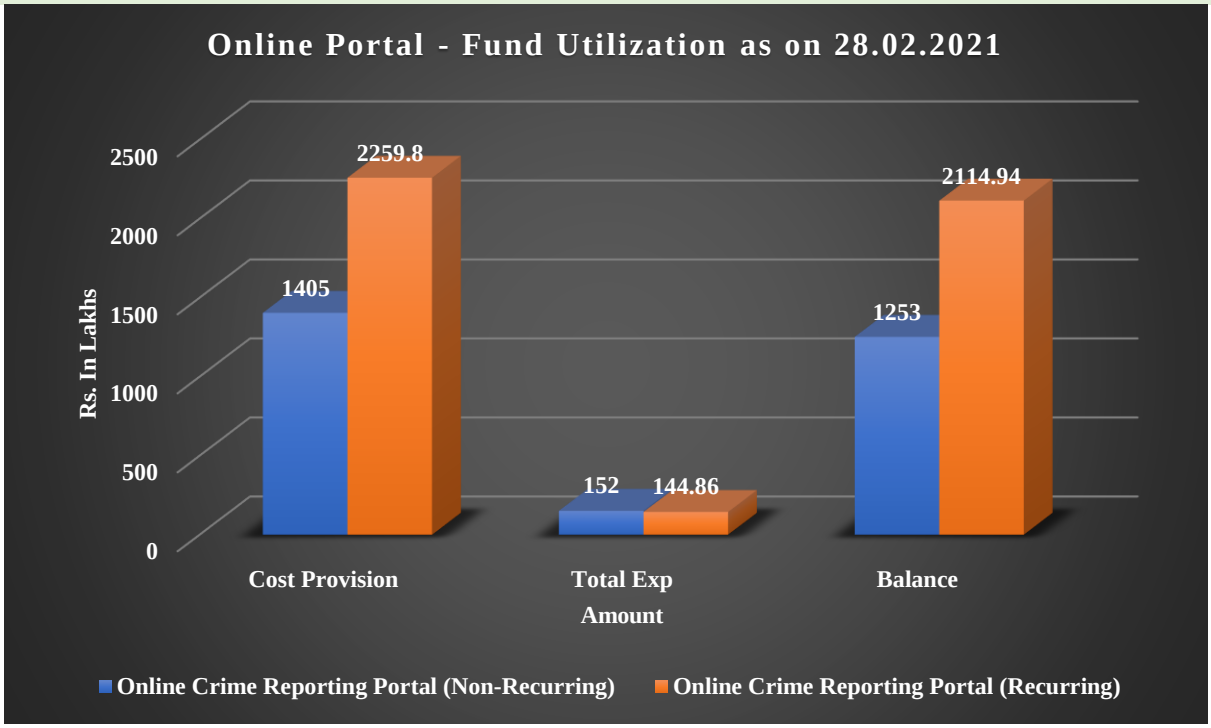


Graph 5 CCPWC Component-wise Expenditure as on 28.02.2021

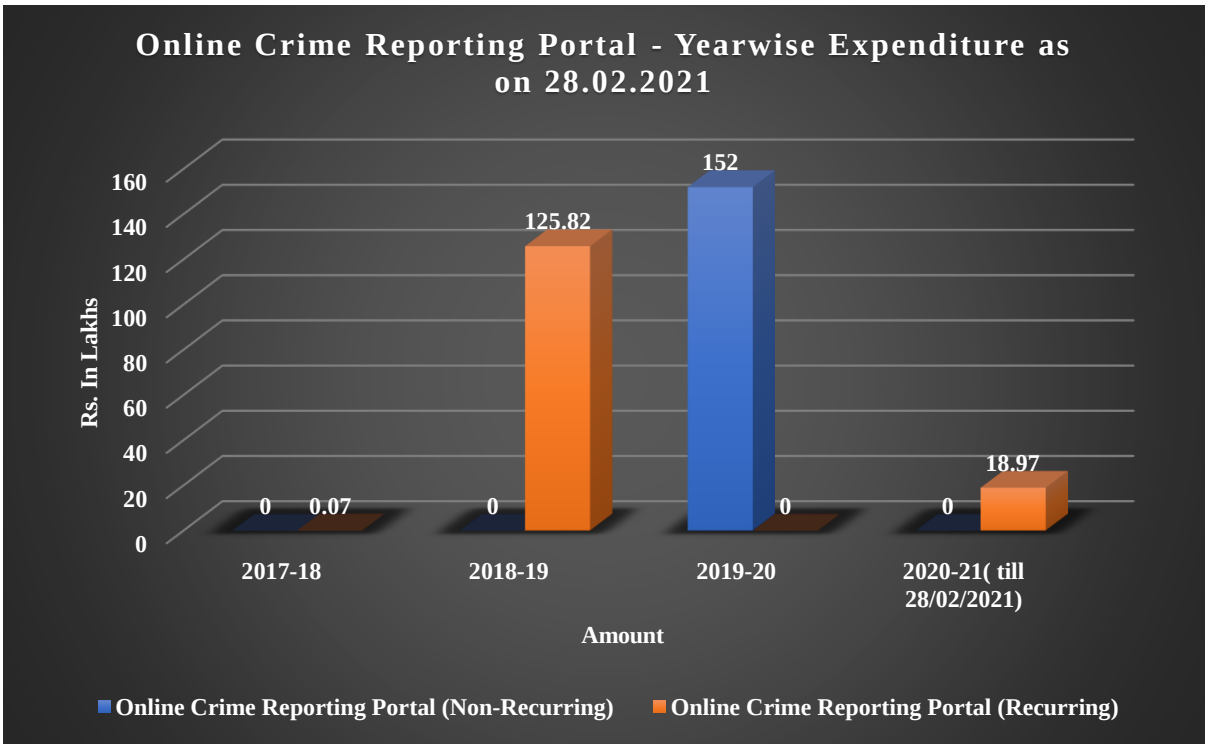
Graph 5 depicts the component-wise total expenditure as booked on 28 February 2021 under the CCPWC scheme. As on date, a total of Rs. 296.86 lakhs (i.e.,**1.33%**) have been spent on operationalizing the Online Cybercrime Reporting Portal. A total of Rs. 553.42 lakhs (**2.48%**) have been spent on establishing the national level forensic laboratory, NCFL(E) in Hyderabad. A total of Rs. 9474.08 lakhs (**42.45%**) have been spent on capacity building in different States/UTs. A total of Rs. 172.66 lakhs (**0.77%**) have been spent on carrying out research and development (R&D) activities. A total of Rs. 617.92 (**2.77%**) lakhs have been spent on spreading awareness across the country. A total of Rs. 534.19 lakhs (**2.39%**) have been spent on operationalizing Project Management Unit (PMU).

3.2. Component-Wise Fund Allocation & Utilization

3.2.1. Online Cybercrime Reporting Platform



Graph 7 Online Portal - Fund Utilization as on 28.02.2021



Graph 6 Online Portal - Year wise Expenditure as on 28.02.2021

Table 9 Online Portal - Expenditure distribution under different Heads

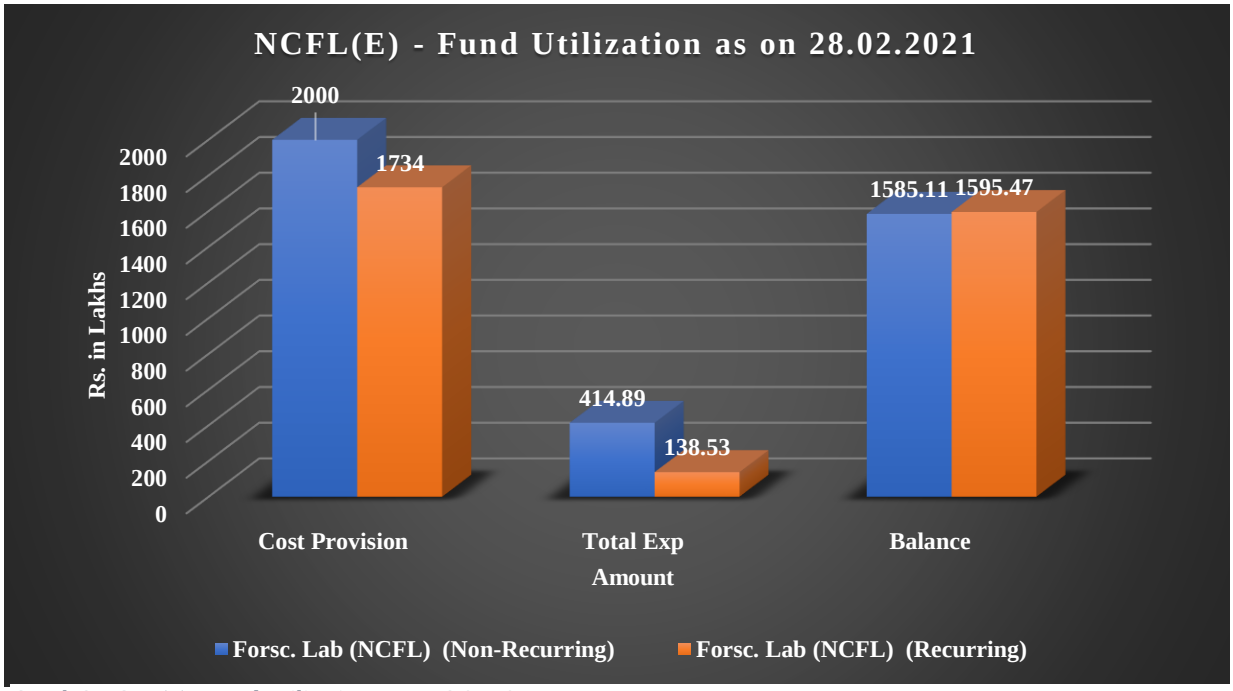
Portal - Expenditure Heads	**2017-18**	**2018-19**	**2019-20**	**2020-21 (28.02.2021)**	**Total Expenditure**
WIPRO-SRS sign off Wipro (15%) -Portal		4.44			4.44
		27			27
Payment to NCRB for procurement of items		83.67	152		235.67
		10.72			10.72
Recurring				18.97	18.97
Grand Total (in Rs. Lakhs)	**0**	**125.83**	**152**	**18.97**	**296.8**

Graphs 6 and **7** depicts the fund allocation and utilization under the Online Cybercrime Reporting Portal component of the CCPWC scheme. As on 28.02.2021, the component has been allocated a total of Rs. 3664.8 lakhs. And the total expenditure incurred is Rs. 296.86 lakhs i.e., **8.10 %** of the total allocated amount.

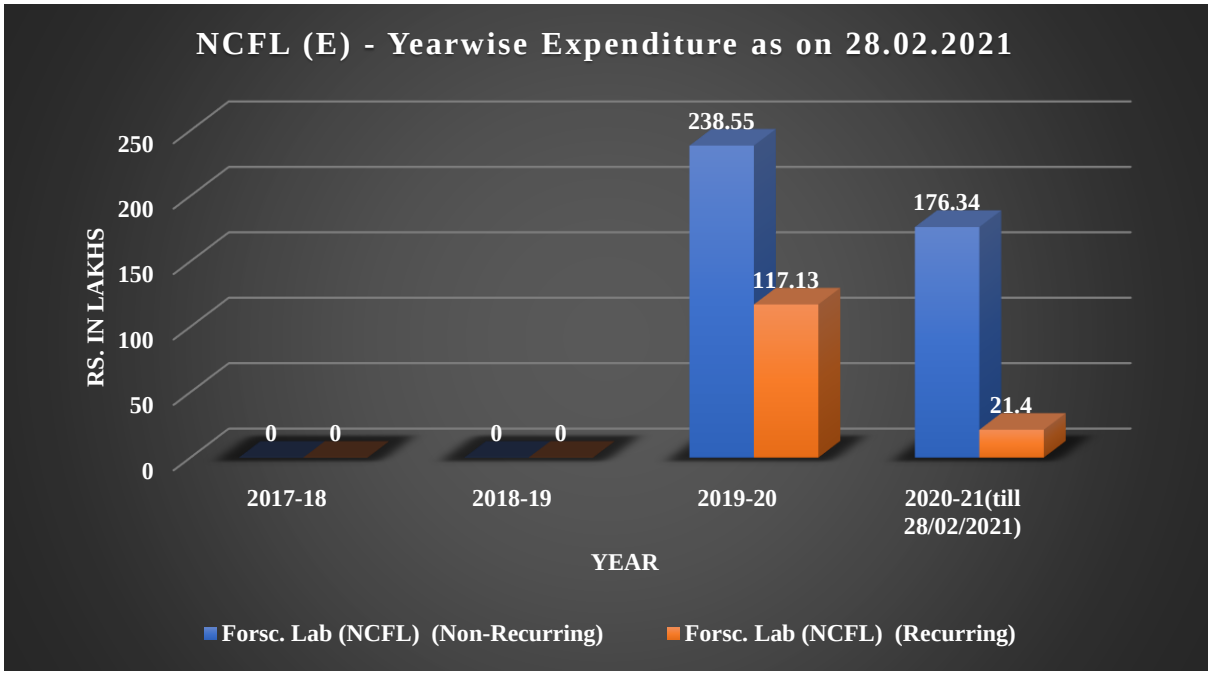
Table **9** shows the distribution of total expenditure incurred under the component. The year 2017-18 did not see any expenditure since the scheme has been newly launched and the portal was in the conceptual stage. The following year i.e., 2018-19, the expenditure incurred was to the tune of Rs. 125.83 lakhs i.e., **42.39 %** of the total expenditure. The same year, the portal was launched in the month of September.

In the year 2019-20, the expenditure incurred was the highest of all, amounting to Rs. 152 lakhs i.e., **51.20 %** of the total expenditure. The expenditure pertained to procurement of equipment by NCRB for the portal. However, the year 2020-21 has seen the least spending, an amount of Rs. 18.97 lakhs i.e., **6.40 %** of the total expenditure as on 28.02.2021. The expenditure pertained to mostly recurring activities.

3.2.2. NCFL (E)



Graph 8 NCFL(E) - Fund Utilization as on 28.02.2021



Graph 9 NCFL (E) Year wise Total Expenditure

Graph 8 and **9** depicts the fund allocation and utilization under the national level forensic laboratory component of CCPWC Scheme. The national level lab has been established at CFSL, Hyderabad under the aegis of DFSS, New Delhi. The total expenditure incurred as on 28 February 2021 is Rs. 553.42 lakhs i.e., **14.82 %** of the total allocated amount i.e., Rs. 3734 lakhs. The expenditure pertains to procurement of hardware/software tools, hiring of 37 technical professionals for the Lab and other operational expenditure.

List of Activities undertaken at the Laboratory :

- Digital Storage Media Examination – Examination of various storage media
- Mobile Phone and Embedded System Examination – Examination of mobile phones and flash media
- Advanced Digital Forensic Examination – Extraction of from Damaged hard disks and mobile phones.
- Scene of Crime – Assisting the LEAs in search, seizure, and preservation of digital evidence.
- The police seized digital exhibits in connection with cybercrimes reported. All the digital exhibits submitted to the laboratory analysed for the probative information and the report is submitted.
- The experts also attended the various Hon'ble courts of law to testify the reports submitted by the laboratory.

List of the equipment to be procured for the Laboratory:

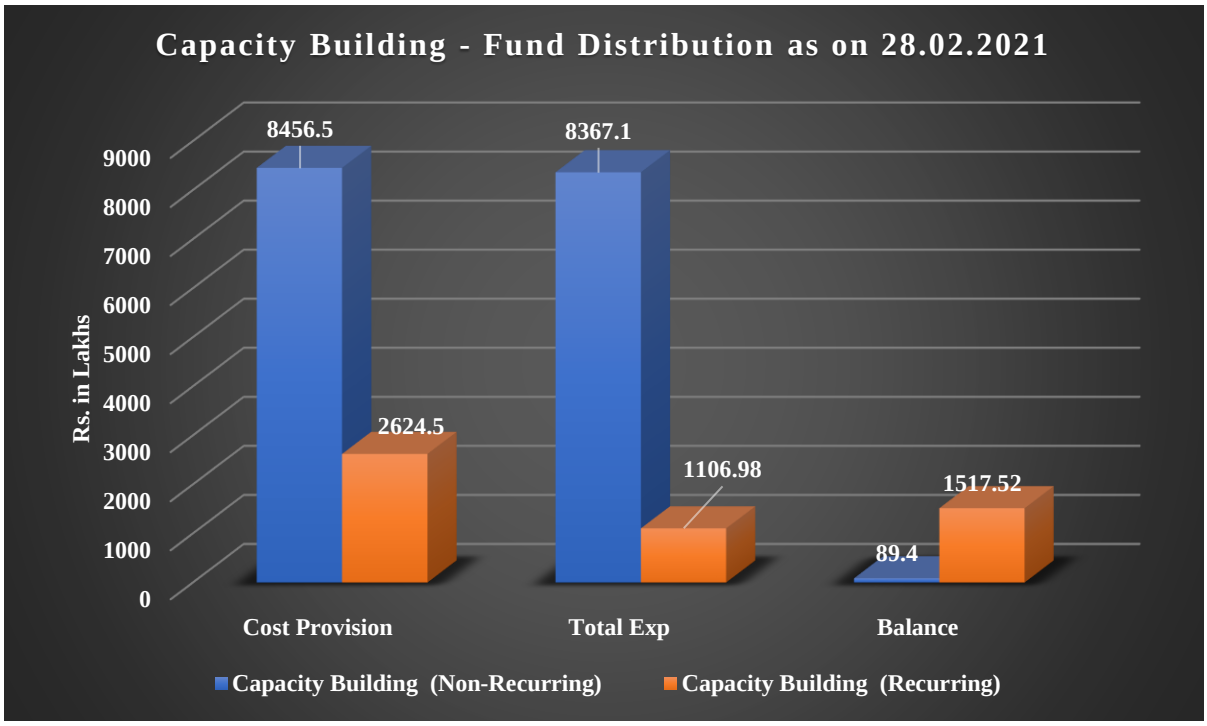
Table 10 List of the equipment to be procured for the Laboratory.

S. No.	Name of the item
1.	Crime Scene Vehicle
2.	SPEKTOR Incident Response Tool
3.	Mobile Forensic Workstations
4.	H/w based Forensic Imaging and Write Blocking Device
5.	H/w based Forensic Imaging Device
6.	H/w based Write Blocker Kit
7.	MAGNET AXIOM
8.	BelkaSoft
9.	EnCase
10.	OS Forensics
11.	FTK
12.	MAC Forensic Tool Kit along with MAC Work Station
13.	Paraben Network Email Examiner
14.	Word Recovery
15.	Excel Recovery
16.	SQL Recovery
17.	SQL LOG Analyser

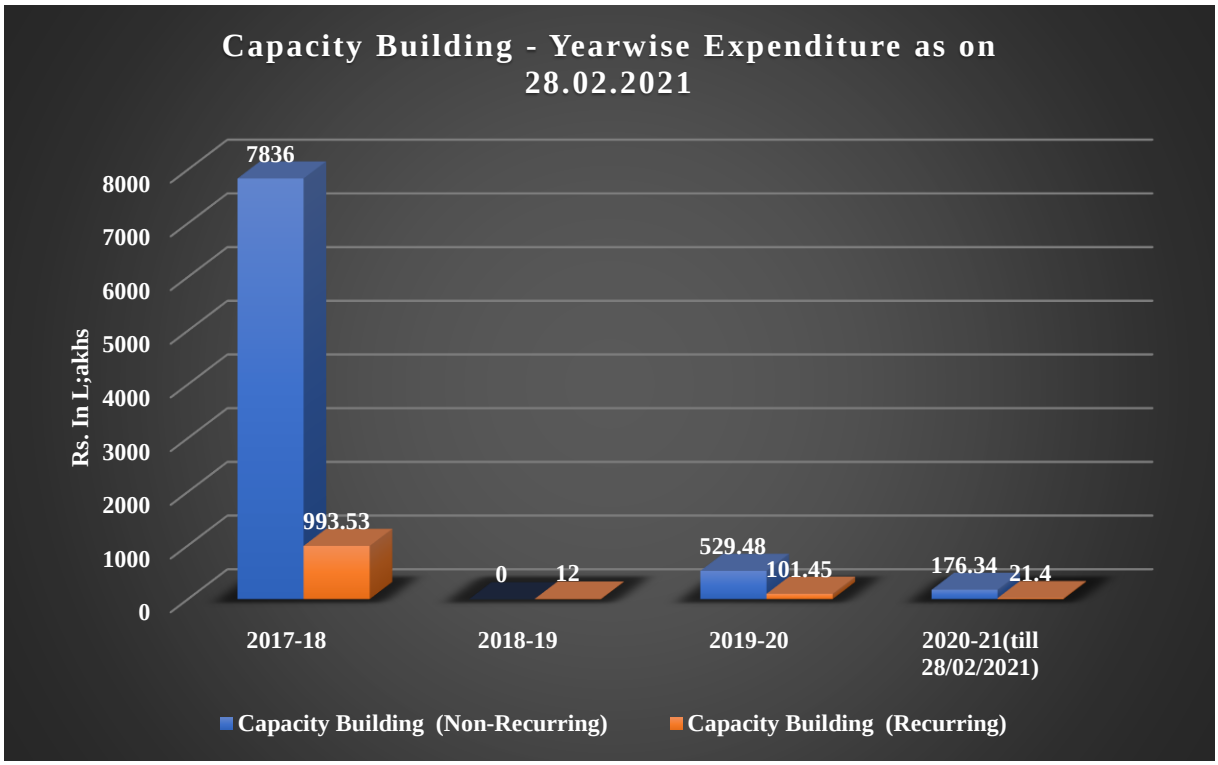
18.	MS Office Suit
19.	High-end Forensic Work Station
20.	TEEL Technologies CHIP OFF
21.	UFED TOUCH2
22.	Forensic Workstations
23.	Passware KIT Forensic
24.	VMware for Windows and MAC
25.	Resource Tuner
26.	Araxis Mearge
27.	REDGate SQL Bundle
28.	LOG Lizard Parser
29.	Thin Clients
30.	Servers for 04 CFSLs

3.2.3. Capacity Building

I. Capacity Building – Overall Fund Allocation and Utilization



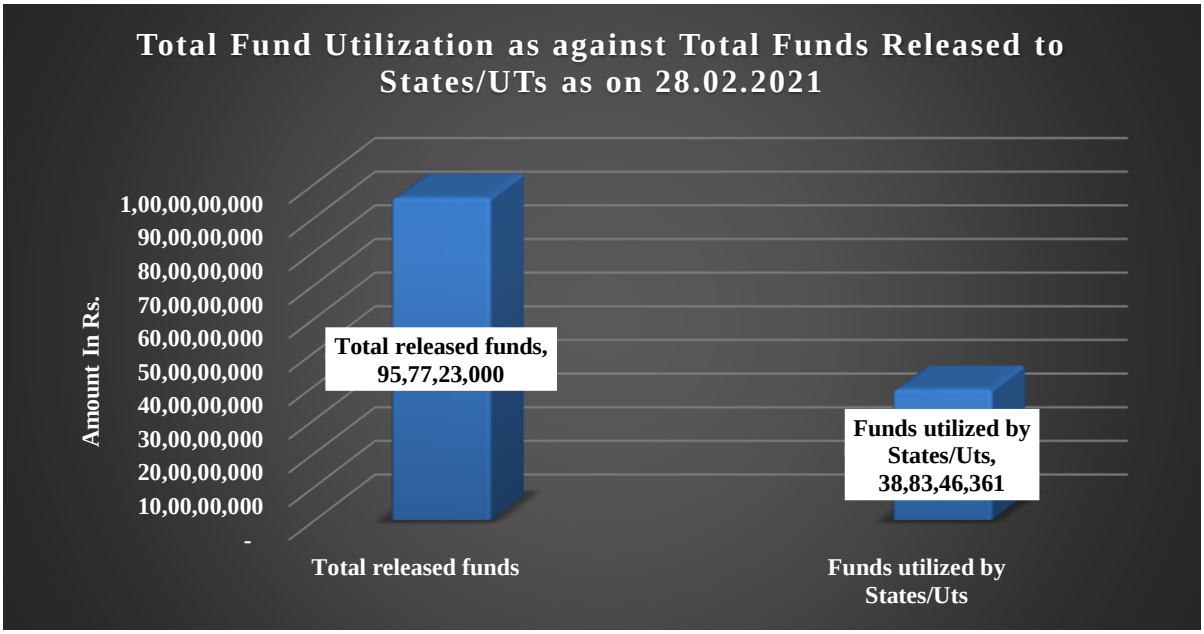
Graph 10 Capacity Building - Fund Distribution as on 28.02.2021



Graph 11 Capacity Building - Year wise Expenditure as on 28.02.2021

Table 11 Capacity Building – Fund Distribution

Year	Forensic Lab	Training	Jr. Cyber Forensic Consultant	Total
2017-18	828000000	60003000	43200000	931203000
2018-19*				
2019-20&	17650000	8870000	0	26520000
2020-21#				
Grand Total	**845650000**	**68873000**	**43200000**	**957723000**
***Funds not utilized in 2017-18, revalidated in 2018-19, again withdrawn in 2018-19**				
&Amount revalidated during FY 2019-20.				
A & N Islands	14800000	175000	1200000	16175000
Chandigarh	14800000	75000	1200000	16075000
Lakshadweep	14800000	0	0	14800000
#Amount revalidated during FY 2020-21				
A & N Islands	9111645	165100	1200000	10476745



Graph 12 Total Fund Utilization as against Total Funds Released to States/UTs as on 28.02.2021

Graphs 10, 11, and **12** depicts the overall fund allocation and utilization under the Capacity Building component of CCPWC. As on 28.02.2021, the total allocation to States/UTs is Rs. 9577.23 lakhs and the total utilization is Rs. 3883.46 lakhs **i.e., 40.54 %** of the total allocated amount. The total expenditure incurred under the three subcomponents is Rs. 8456.50 lakhs (**88.3%)** for Forensic Lab, Rs. 688.73 lakhs for Training (**7.19%),** and Rs. 432 lakhs **(4.33%)** for Jr. Cyber Consultant.

II. Capacity Building – Category-wise Fund Allocation and Distribution

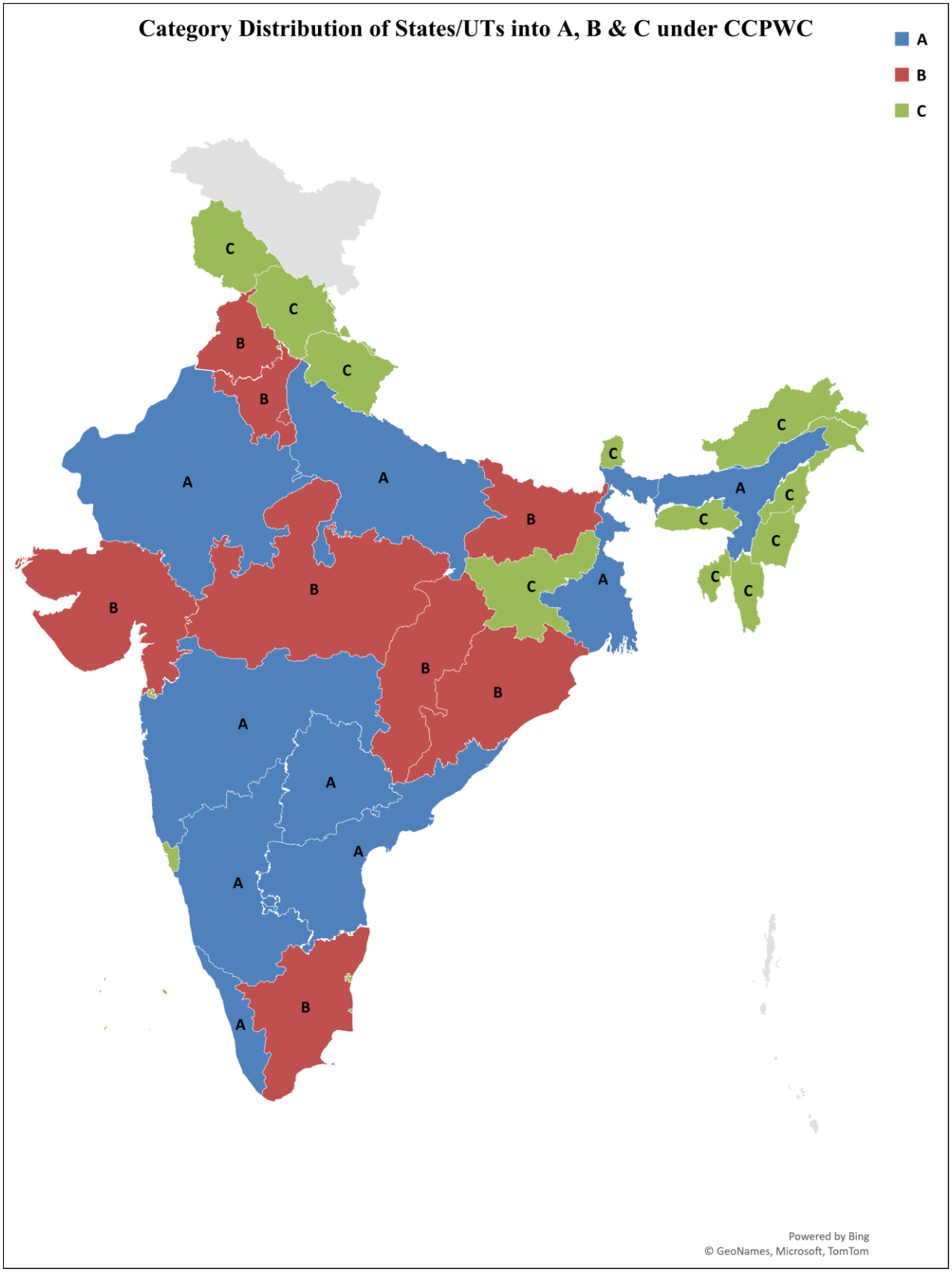
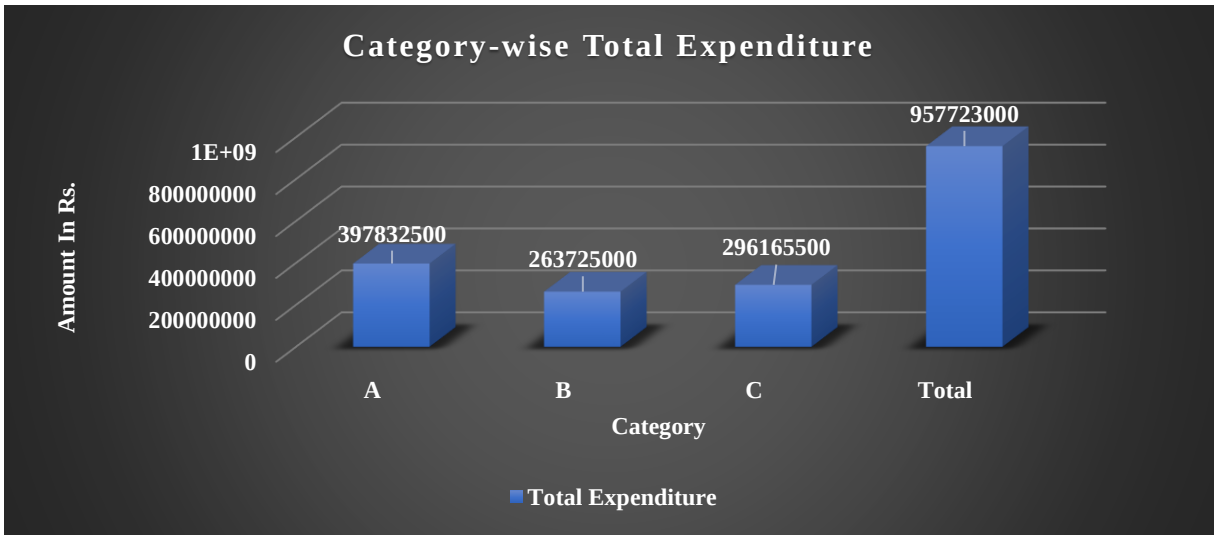


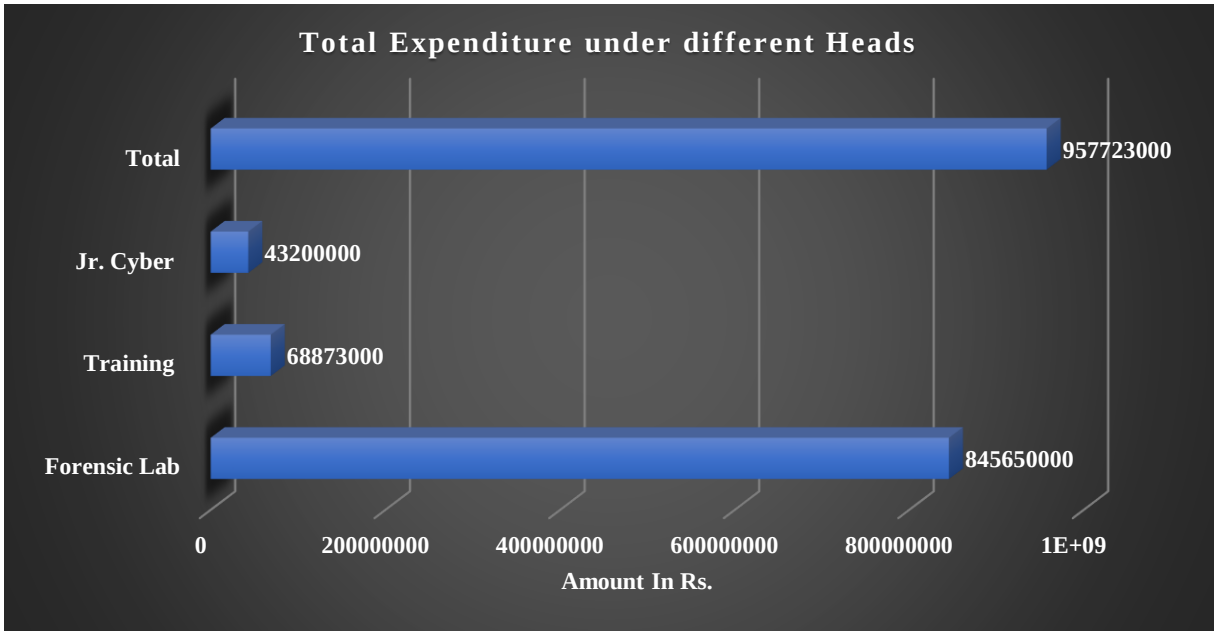
Figure 9 Category Distribution of States/UTs into A, B & C under CCPWC

Figure 10 depicts the distribution of 36 States and UTs into three different categories A, B and C under the CCPWC scheme. There are 9 States/UTs each under the category A and B while there are 18 States/UTs under category C. The categorization of States and UTs has been done based on the number of cybercrime cases reported in each State/UT and the funds are allocated as per number of workstations to be set up in the lab in each State/UT.

Graph 14 depicts the total expenditure incurred under all the categories. As on 28 February 2021, under the scheme, the total allocated amount to all States/UTs is Rs. 9577.23 lakhs. The allocated amount to States/UTs under the Category A is Rs. 3978.32 lakhs (**41.54%),** under the Category B is Rs. 2637.25 lakhs (**27.54%)** and under the Category C is Rs. 2961.65 lakhs (**30.92%).**



Graph 14 Category wise – Total Expenditure



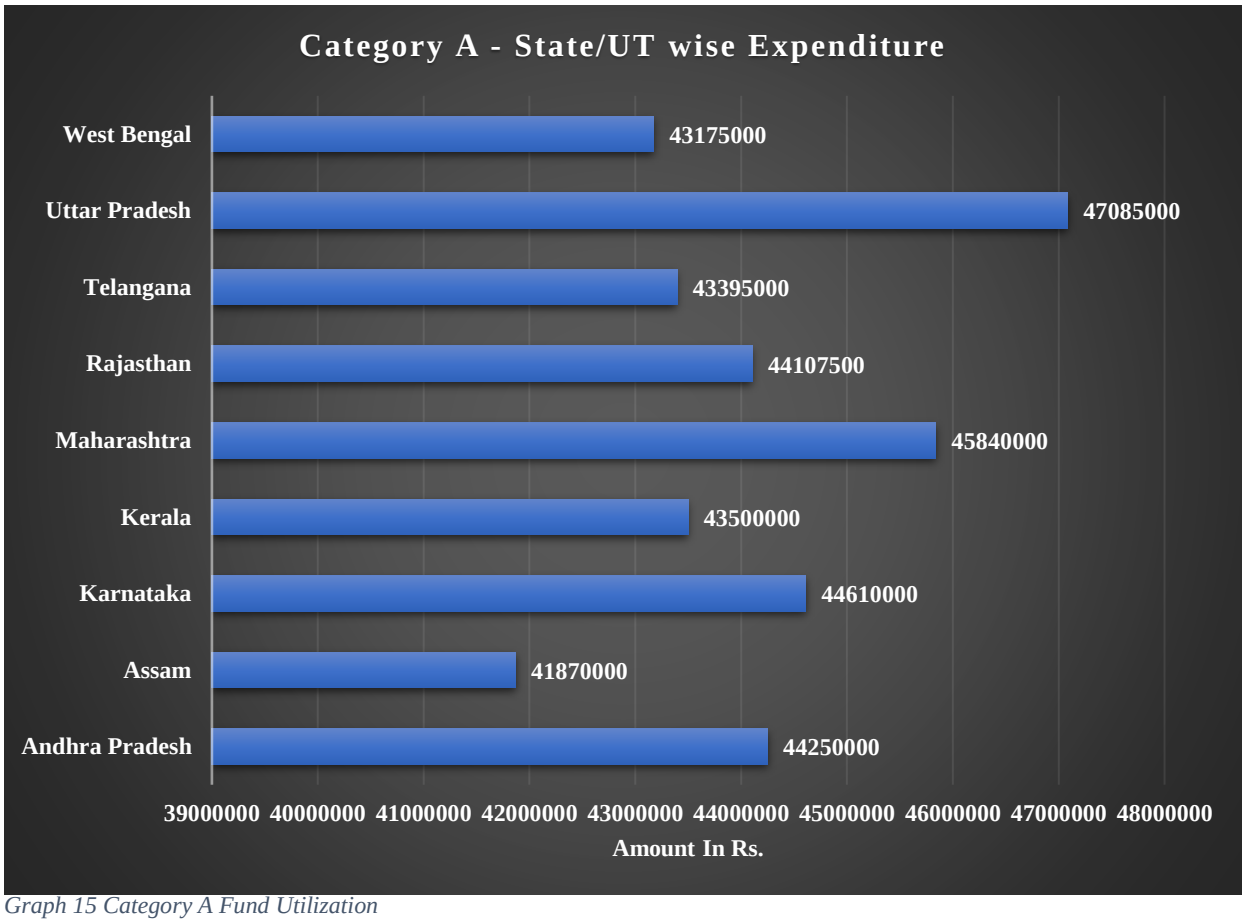
Graph 13 Capacity Building – Expenditure under different heads

Table 12 Fund distribution under different heads of Capacity Building

Category	Forensic Lab	Training	Jr. Cyber Forensic Consultant	Sum (In Rs.)
A	354600000	32432500	10800000	397832500
B	223850000	29075000	10800000	263725000
C	267200000	7365500	21600000	296165500
Total (In Rs.)	**845650000**	**68873000**	**43200000**	**957723000**

Graph 13 and **Table 12** represent the fund distribution under different sub-components of Capacity building in States/UTs. The three subcomponents, namely, establishing forensic labs in each State/UT, Training, and Hiring of Jr. Cyber Forensic Consultant have been allocated Rs. 8456.50 lakhs, Rs. 688.73 lakhs, and Rs. 432 lakhs, respectively.

1. Category A - Fund Allocation



Graph 15 Category A Fund Utilization

Graph 15 depicts the fund distribution to States/UTs in the Category A. There are a total of 9 States in the category and the total allocation is Rs. 3978.32 lakhs.

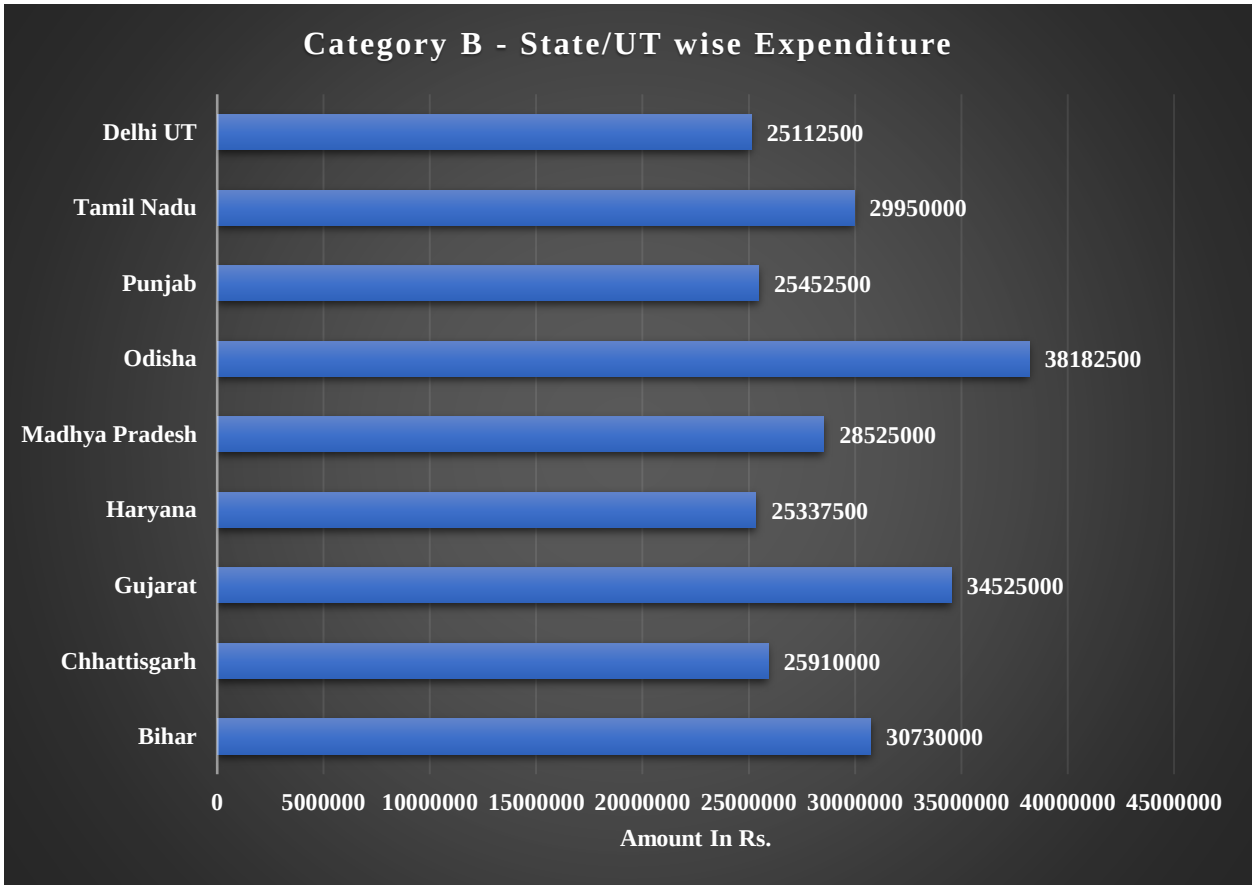
The State/UT-wise fund allocation under Category A (in descending order) is as follows:

Table 13 Category A-State/UT wise Fund Allocation

State/UT	Category	Forensic Lab	Training	Jr. Cyber Forensic Consultant	Sum (In Rs.)
Uttar Pradesh	A	39400000	6485000	1200000	47085000
Maharashtra	A	39400000	5240000	1200000	45840000
Karnataka	A	39400000	4010000	1200000	44610000
Andhra Pradesh	A	39400000	3650000	1200000	44250000
Rajasthan	A	39400000	3507500	1200000	44107500
Kerala	A	39400000	2900000	1200000	43500000
Telangana	A	39400000	2795000	1200000	43395000
West Bengal	A	39400000	2575000	1200000	43175000
Assam	A	39400000	1270000	1200000	41870000
Grand Total (In Rs.)		**354600000**	**32432500**	**10800000**	**397832500**

Table 13 tabulates the respective allocation to different States/UTs in Category A in descending order. Uttar Pradesh has received the highest allocated amount of Rs. 470.85 lakhs, followed by Maharashtra i.e., Rs. 458.40 lakhs, Karnataka i.e., Rs. 446.10 lakhs , and Andhra Pradesh i.e., Rs. 442.50 lakhs. Allocated amounts to other states are as follows: Rajasthan (Rs. 441.07 lakhs), Kerala (Rs. 435 lakhs) , Telangana (Rs. 433.95 lakhs), and West Bengal (Rs. 431.75 lakhs). The lowest amount of allocation under this category has been to the state of Assam i.e., Rs. 418.70 lakhs. The total allocation under the Category A is Rs. 3978.32 lakhs.

2. Category B – Fund Allocation



Graph 16 Category B Fund Utilization

Graph 16 depicts the fund distribution to States/UTs in the Category B. There are a total of 9 States in this category and the total allocation is Rs. 2637.25 lakhs.

The State/UT-wise fund allocation under Category B (in descending order) is as follows:

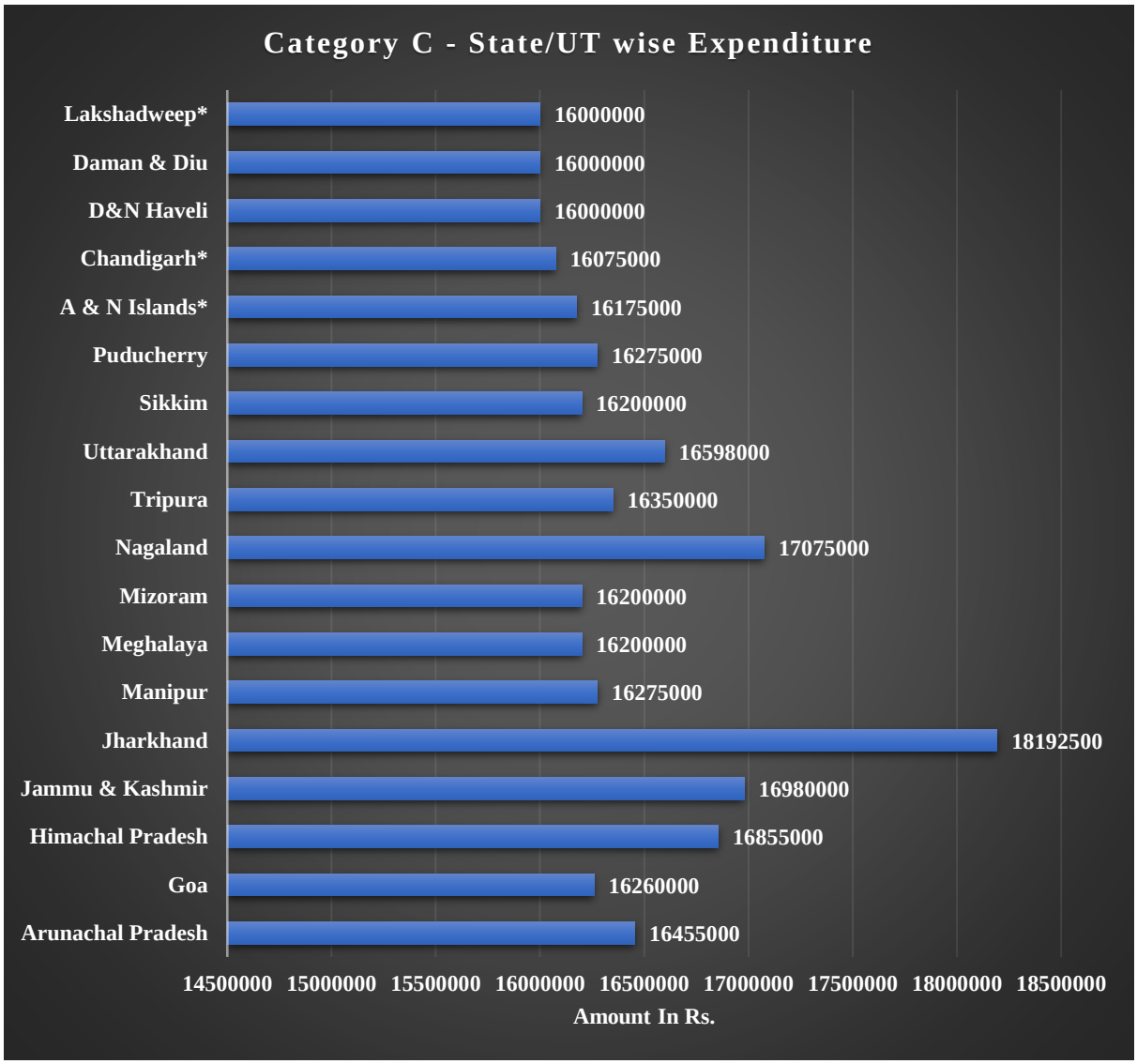
Table 14 Category B-State/UT wise Fund Allocation

State/UT	Category	Forensic Lab	Training	Jr. Cyber Forensic Consultant	Sum (In Rs.)
Odisha	B	35000000	1982500	1200000	38182500
Gujarat	B	27850000	5475000	1200000	34525000
Bihar	B	23000000	6530000	1200000	30730000
Tamil Nadu	B	23000000	5750000	1200000	29950000
Madhya Pradesh	B	23000000	4325000	1200000	28525000
Chhattisgarh	B	23000000	1710000	1200000	25910000

Punjab	B	23000000	1252500	1200000	25452500
Haryana	B	23000000	1137500	1200000	25337500
Delhi UT	B	23000000	912500	1200000	25112500
Grand Total (In Rs.)		**223850000**	**29075000**	**10800000**	**263725000**

Table 14 tabulates the respective allocation to different States/UTs in Category B in descending order. Odisha has received the highest allocated amount of Rs. 381.82 lakhs, followed by Gujarat i.e., Rs. 345.25 lakhs, Bihar i.e., Rs. 307.30 lakhs , and Tamil Nadu i.e., Rs. 299.50 lakhs. Allocated amounts to other states are as follows: Madhya Pradesh (Rs. 285.25 lakhs), Chhattisgarh (Rs. 259.10 lakhs) , Punjab (Rs. 254.52 lakhs), and Haryana (Rs. 253.37 lakhs). The lowest amount of allocation under this category has been to the UT of Delhi i.e., Rs. 251.12 lakhs. The total allocation under the Category B is Rs. 2637.25 lakhs.

3. Category C – Fund Allocation



Graph 17 Category C Fund Allocation

Graph 17 depicts the fund distribution to States/UTs in the Category C. There are a total of 18 States in this category and the total allocation is Rs. 2961.65 lakhs.

The State/UT-wise fund allocation under Category C (in descending order) is as follows:

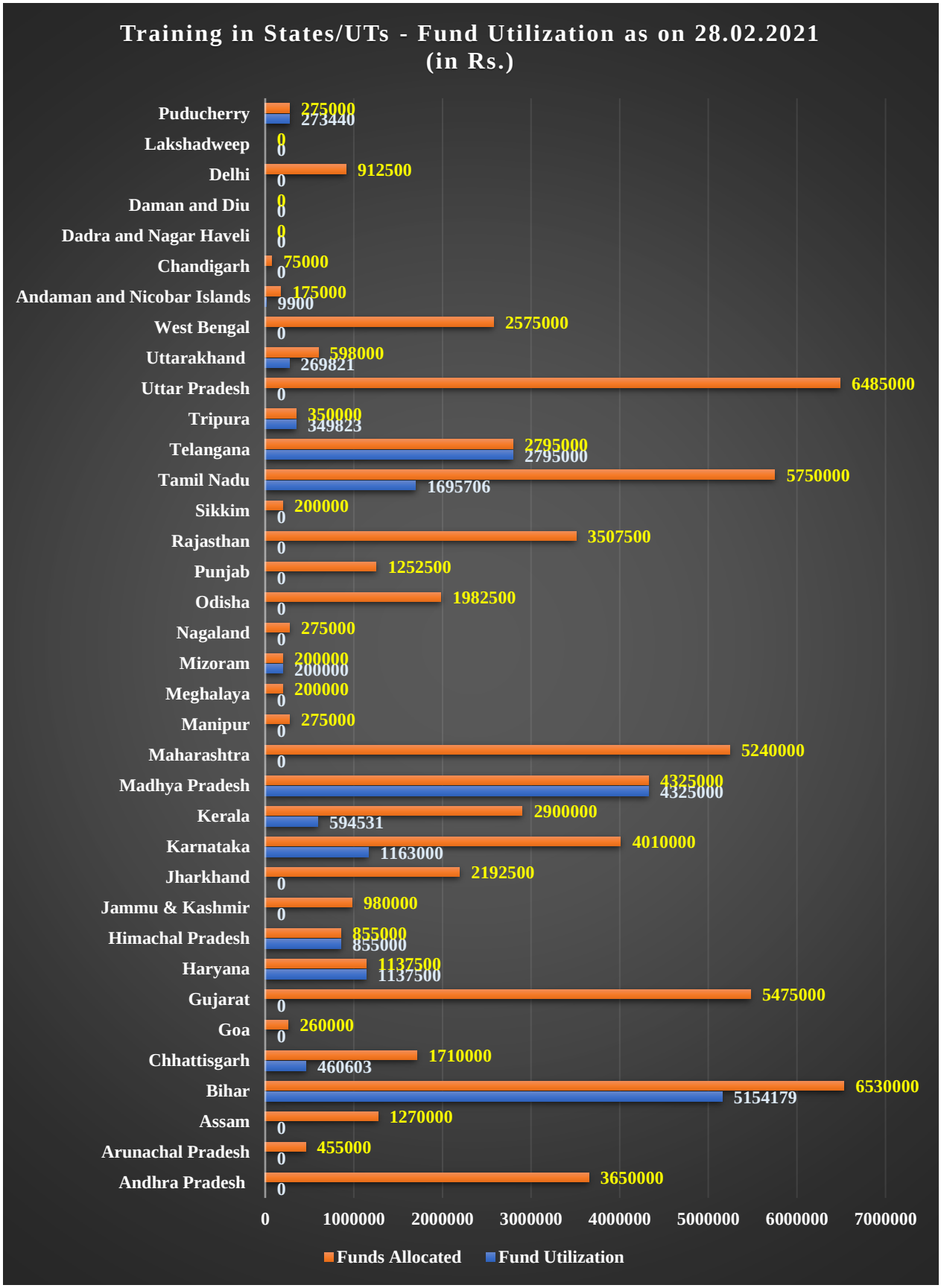
Table 15 Category C-State/UT wise Fund Allocation

State/UT	Category	Forensic Lab	Training	Jr. Cyber Forensic Consultant	Sum (In Rs.)
Jharkhand	C	14800000	2192500	1200000	**18192500**
Nagaland	C	15600000	275000	1200000	**17075000**

Jammu & Kashmir	C	14800000	980000	1200000	**16980000**
Himachal Pradesh	C	14800000	855000	1200000	**16855000**
Uttarakhand	C	14800000	598000	1200000	**16598000**
Arunachal Pradesh	C	14800000	455000	1200000	**16455000**
Tripura	C	14800000	350000	1200000	**16350000**
Manipur	C	14800000	275000	1200000	**16275000**
Puducherry	C	14800000	275000	1200000	**16275000**
Goa	C	14800000	260000	1200000	**16260000**
Meghalaya	C	14800000	200000	1200000	**16200000**
Mizoram	C	14800000	200000	1200000	**16200000**
Sikkim	C	14800000	200000	1200000	**16200000**
A & N Islands	C	14800000	175000	1200000	**16175000**
Chandigarh	C	14800000	75000	1200000	**16075000**
D&N Haveli	C	14800000	0	1200000	**16000000**
Daman & Diu	C	14800000	0	1200000	**16000000**
Lakshadweep	C	14800000	0	1200000	**16000000**
Grand Total (In Rs.)		**267200000**	**7365500**	**21600000**	**296165500**

Table 15 tabulates the respective allocation to different States/UTs in Category C in descending order. Jharkhand has received the highest allocated amount of Rs. 181.92 lakhs, followed by Nagaland i.e., Rs. 170.75 lakhs, Jammu & Kashmir (Rs.169.80 lakhs), Himachal Pradesh (Rs.168.55 lakhs), Uttarakhand (Rs. 165.98 lakhs), Arunachal Pradesh (Rs.164.55 lakhs), Tripura (Rs.163.50 lakhs), Manipur (Rs.162.75 lakhs), Puducherry (Rs.162.75 lakhs), Goa (Rs. 162.60 lakhs), Meghalaya (Rs. 162 lakhs), Mizoram (Rs.162 lakhs), and Sikkim (Rs. 162 lakhs). The fund allocation to the UTs in this category is as follows: A & N Islands (Rs. 161.75 lakhs), Chandigarh (Rs.160.75 lakhs), D&N Haveli (Rs.160 lakhs), Daman & Diu (Rs. 160 lakhs), and Lakshadweep (Rs.160 lakhs). The total allocation under the Category C is Rs. 2961.65 lakhs.

III. Capacity Building – Training (Fund Allocation and Utilization)



Graph 18 Training in States/UTs - Fund Utilization as on 28.02.2021

Graph 18 depicts the fund allocation and utilisation of States/UTs in respect to trainings being conducted to enhance capacity development of LEAs. Of the total 36 States & UTs, 33 States/UTs have received funding. Further, out of 33, 14 States/UTs have utilized the funds to conduct trainings for LEAs. The fund utilization by the 14 States/UTs is as follows:

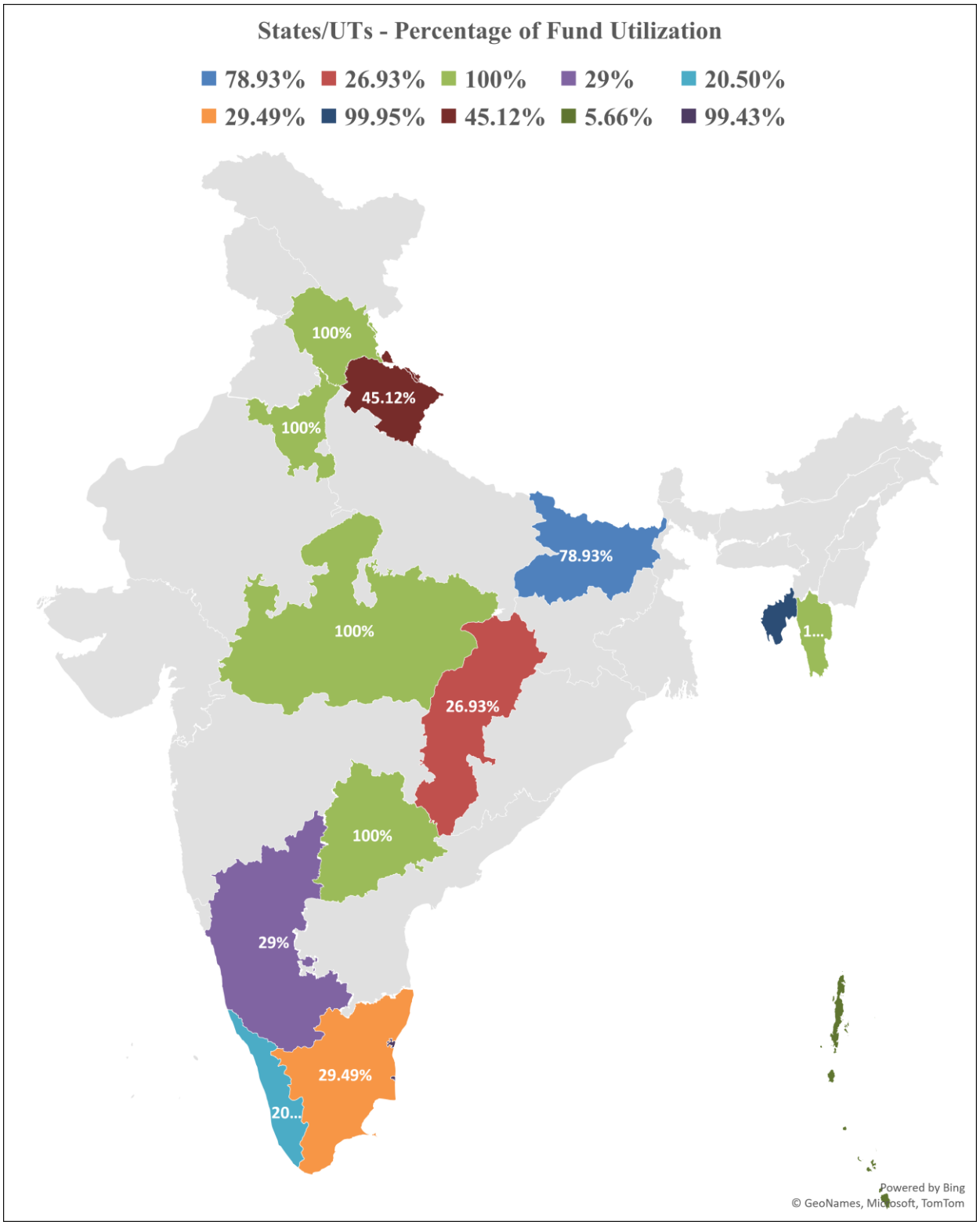
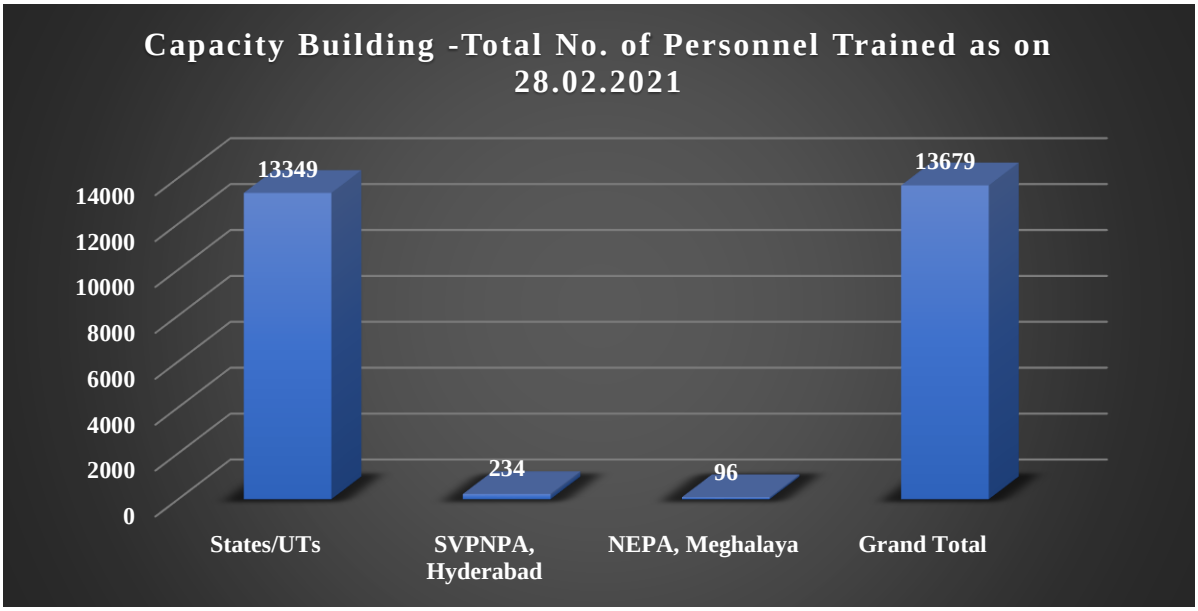
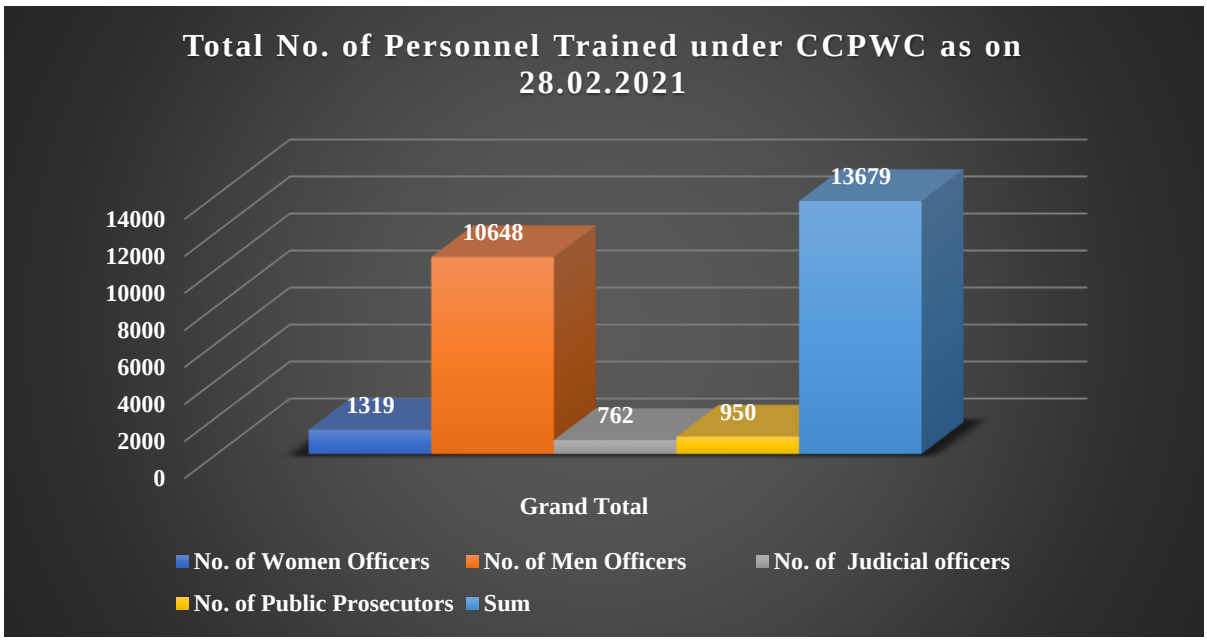


Figure 10 States/UTs - Percentage of Fund Utilization under Trainings

Number of Personnel Trained under different Heads:



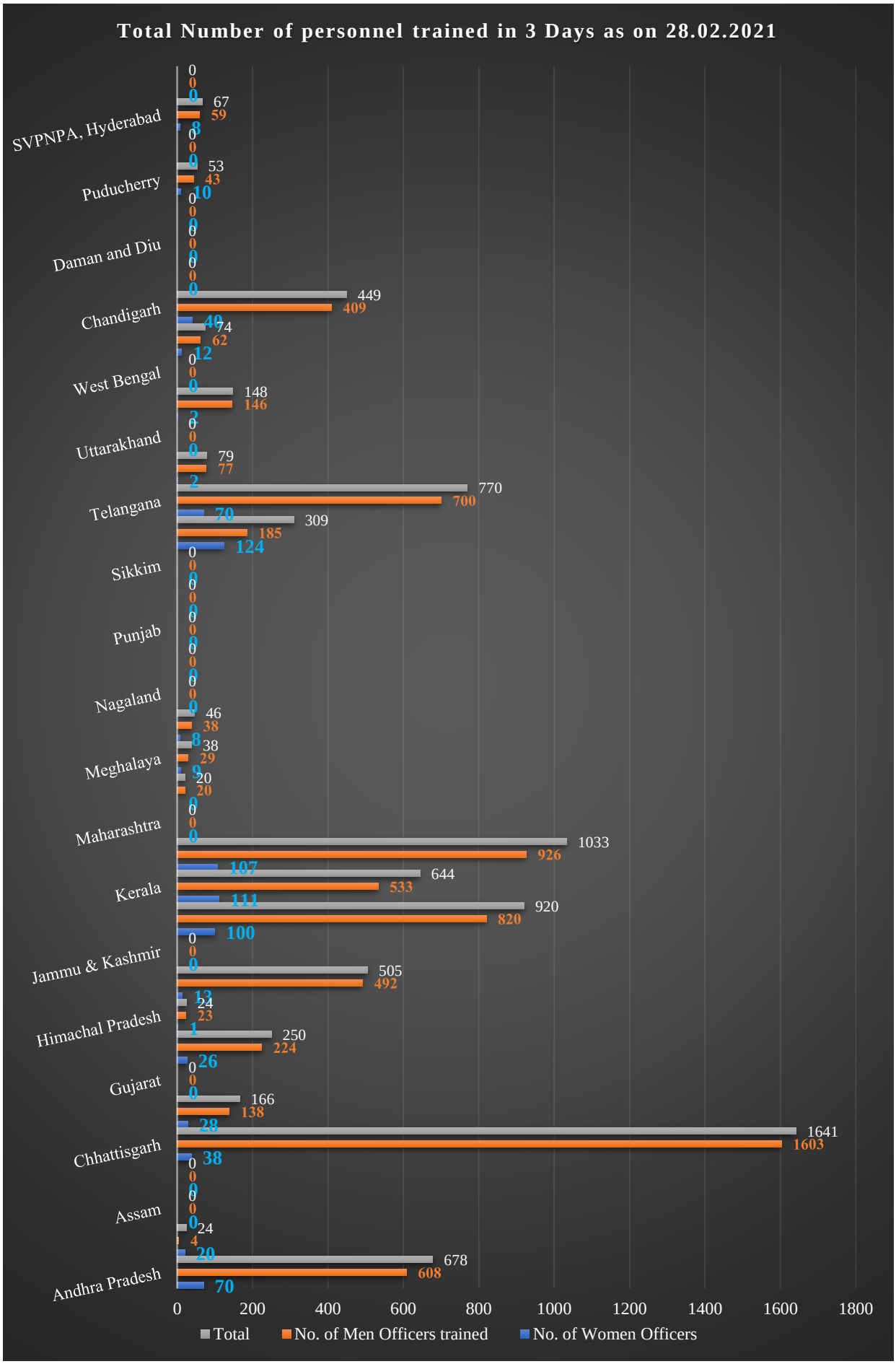
Graph 19 Capacity Building -Total No. of Personnel Trained as on 28.02.2021



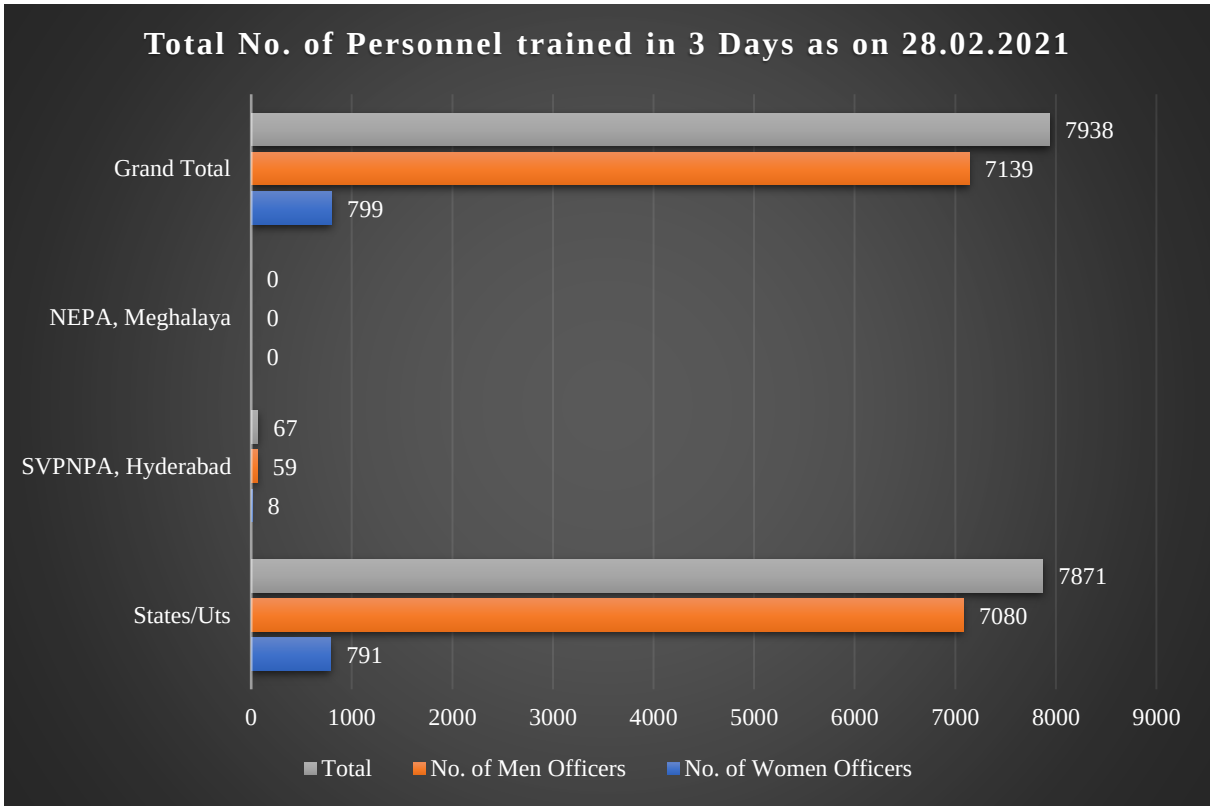
Graph 20 Total No. of Personnel Trained under different heads as on 28.02.2021

Graph 19 and **20** depicts the total number of personnel trained in different States/UTs and the two nodal police training academies i.e., SVPNPA in Hyderabad and NEPA in Meghalaya.

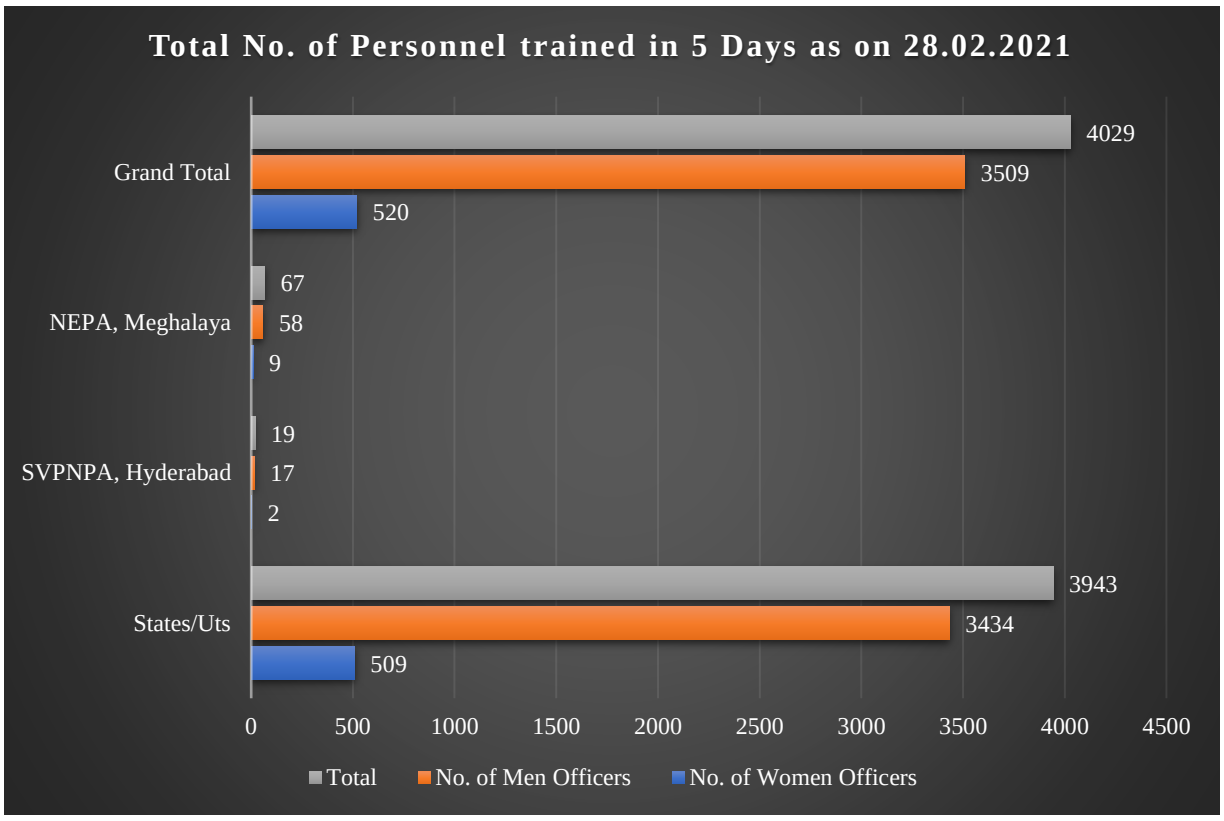
As on 28.02.2021, the total no. of police personnel trained in the States/UTs is **13349**, and in the two academies is **330** (i.e., 234 in SVPNPA and 96 in NEPA). Out of this, total number of women police officers trained is 1319 while total no. of men police officers trained is 10648. The total number of Judicial officers trained is **762** while the total number of Public Prosecutors trained is **950**. Therefore, the grand total no. of personnel trained is 13679. Further, details on personnel training 3 Day and 5 Day training programs are as follows:



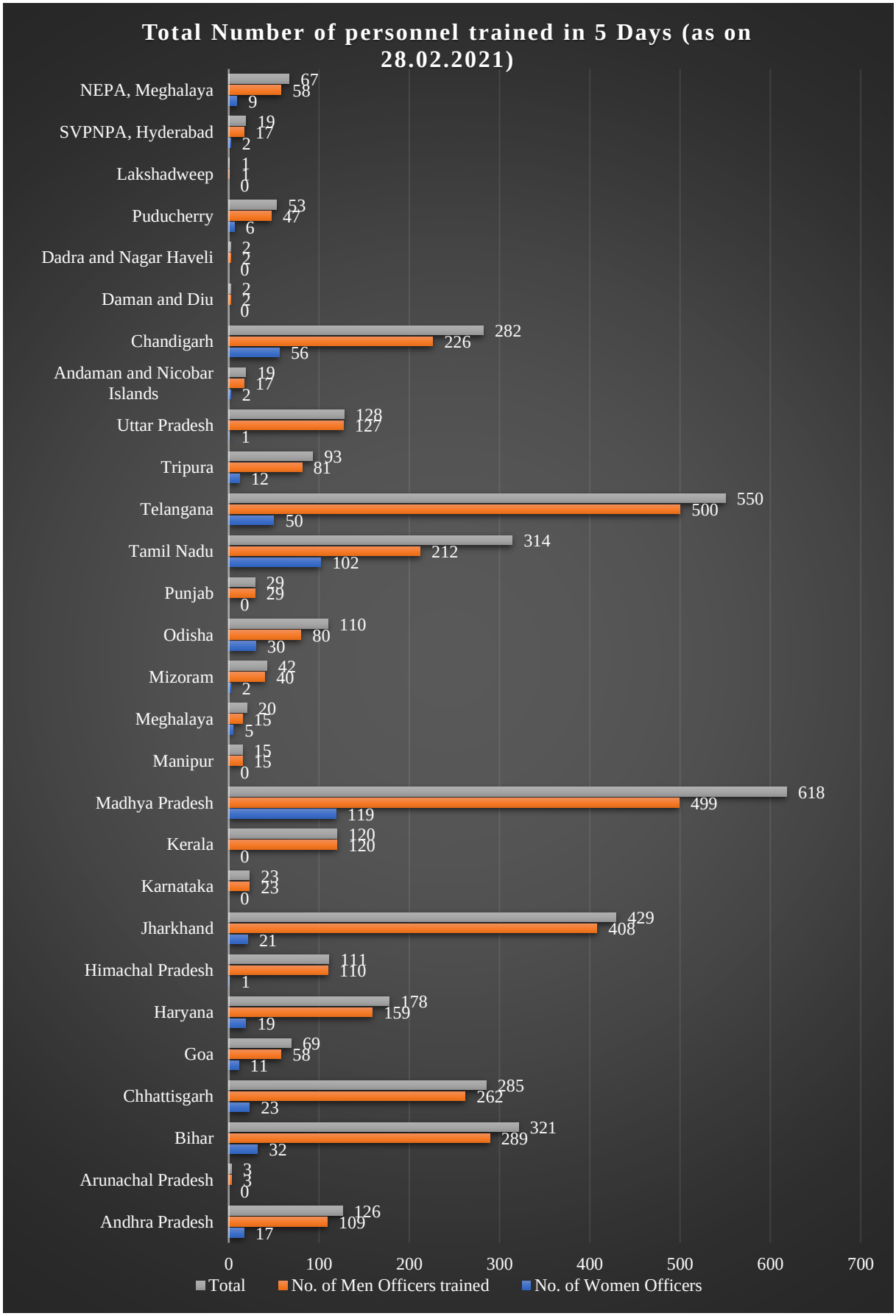
Graph 21 Number of personnel trained in 3 Days as on 28.02.2021



Graph 22 Total No. of Personnel trained in 3 Days as on 28.02.2021

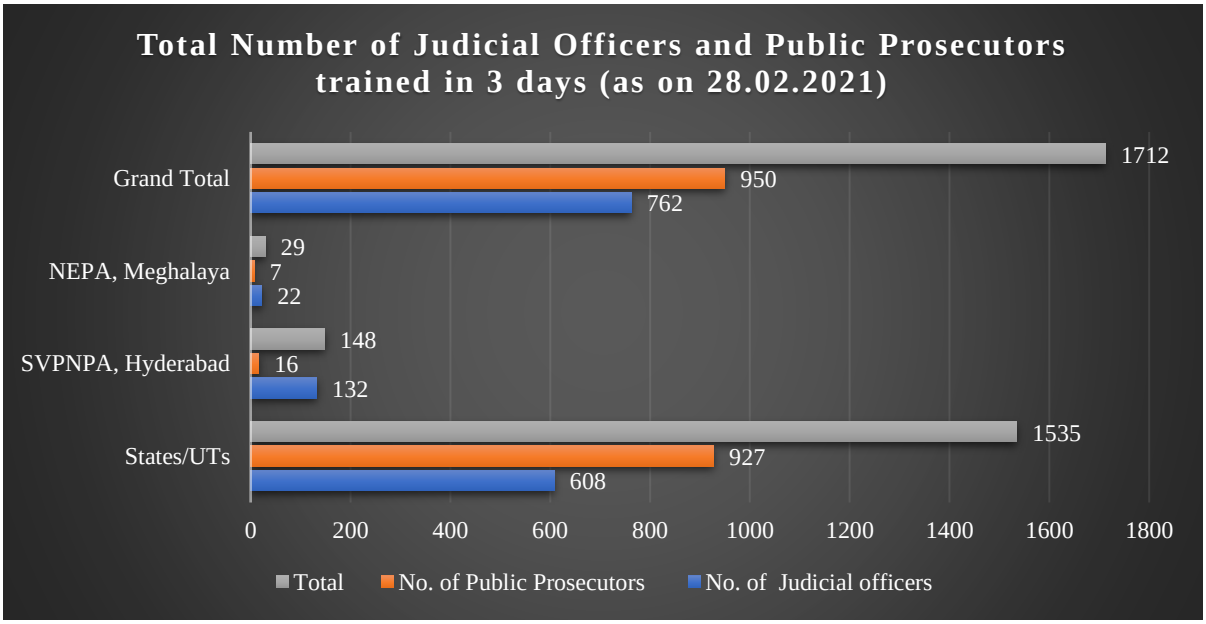


Graph 23 Total No. of Personnel trained in 5 Days as on 28.02.2021



Graph 24 Total Number of personnel trained in 5 Days (as on 28.02.2021)

Graph 21 and **22** depicts the number of personnel trained in 3 days training programs. As on 28.02.2021, the total number of personnel trained is 7938 which includes 7139 men police officers and 799 women police officers. Graph 23 and 24 depicts the number of personnel trained in 5 days training programs. As on 28.02.2021, a total number of 4029 personnel have been trained which includes 3509 men police officers and 520 women police officers.

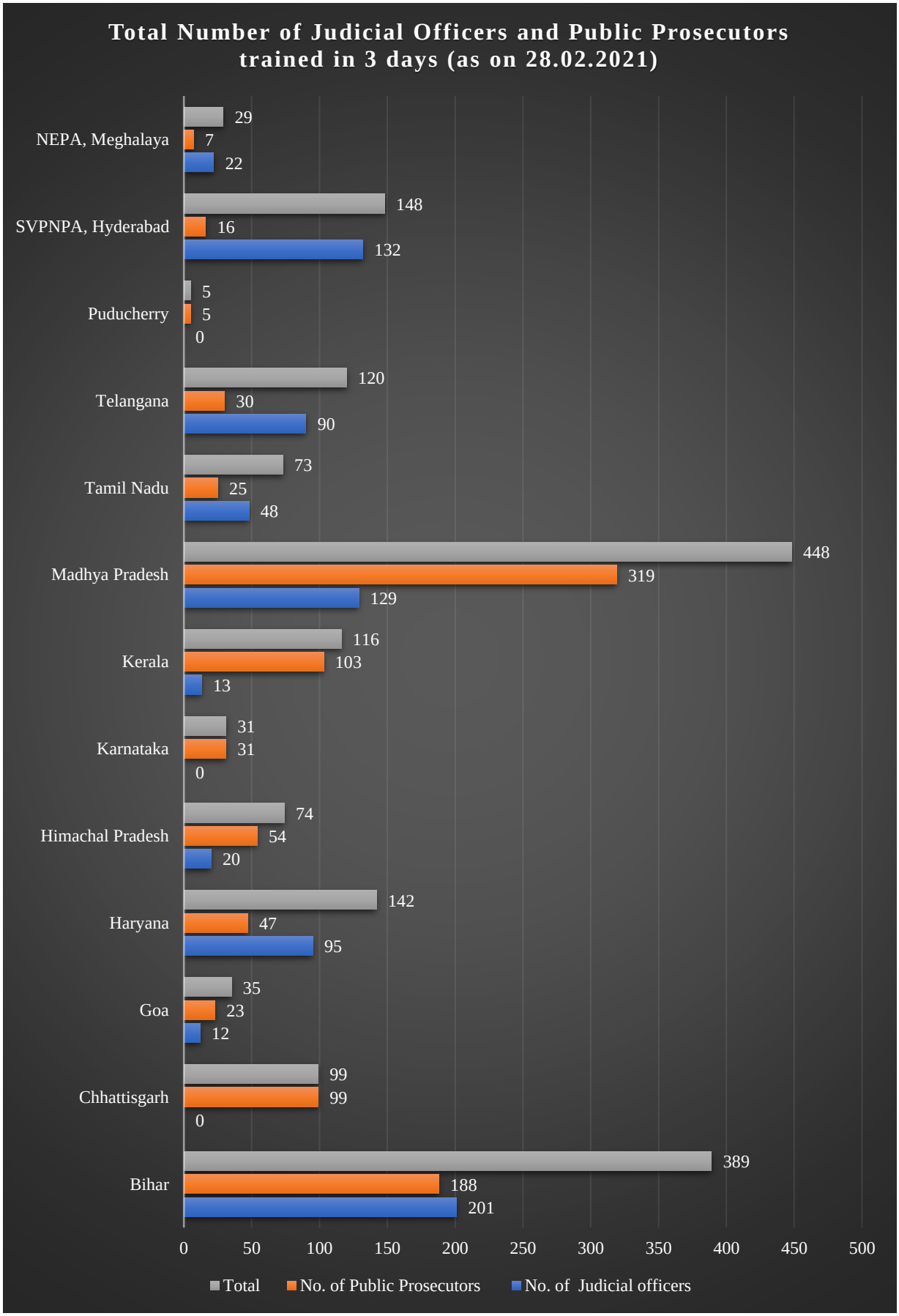


Graph 25 Total Number of Judicial Officers and Public Prosecutors trained in 3 days (as on 28.02.2021)

Table 16 Total No. of Judicial Officers and Public Prosecutors Trained

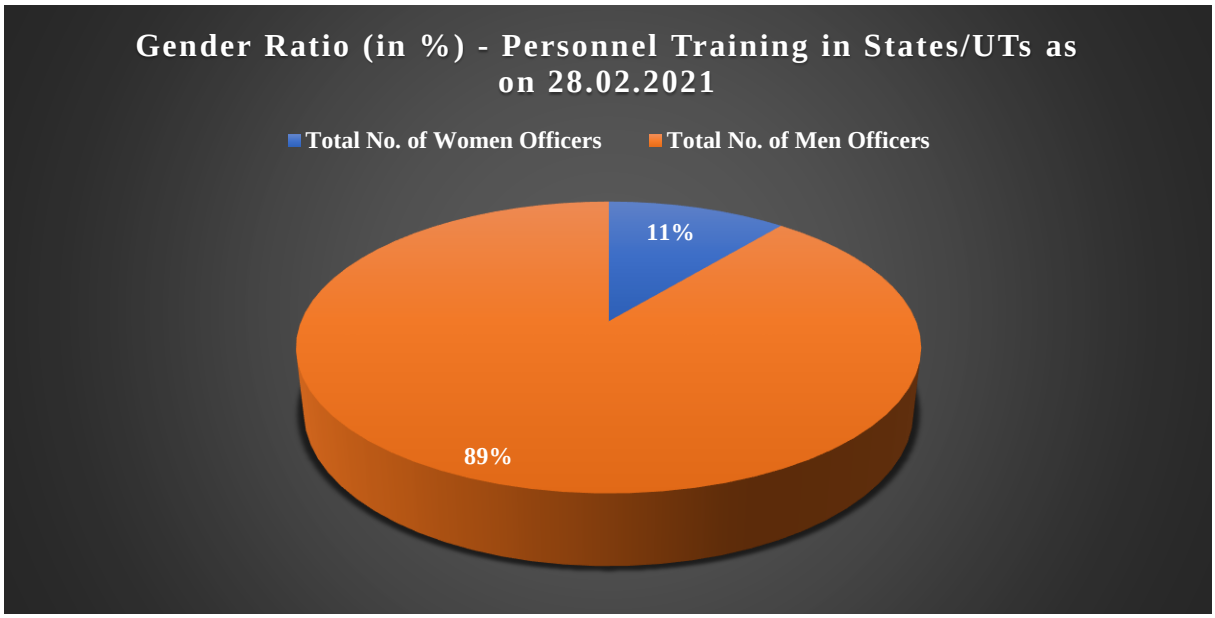
No. of Personnel Trained	Total No. of Judicial officers	Total No. of Public Prosecutors	Total
States/UTs	608	927	**1535**
SVPNPA, Hyderabad	132	16	**148**
NEPA, Meghalaya	22	7	**29**
Grand Total	**762**	**950**	**1712**

Graph 25 depicts the total number of Judicial officers and Public Prosecutors trained in 3-day training programs. As on 28.02.2021, a total number of 1712 personnel have been trained, i.e., 950 Public Prosecutors and 762 Judicial Officers. Further details of training in each state or UT and academy are depicted in **Graph 26** on the next page.

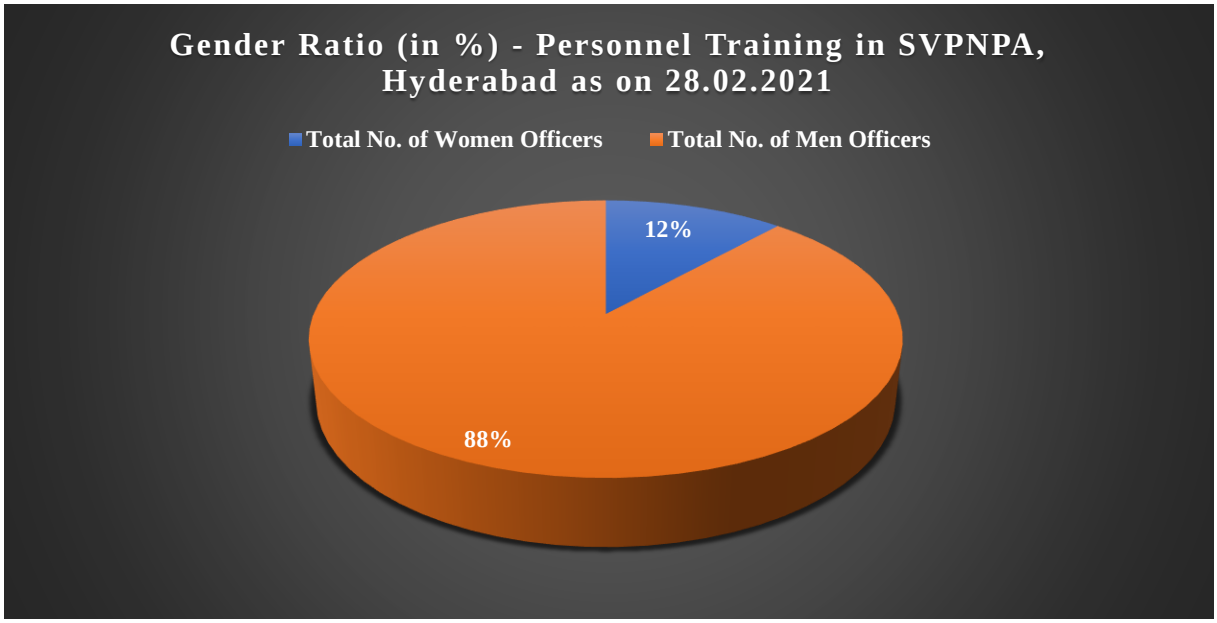


Graph 26 Total Number of Judicial Officers and Public Prosecutors trained in 3 days (as on 28.02.2021)

Gender Ratio Analysis of Capacity Building Training



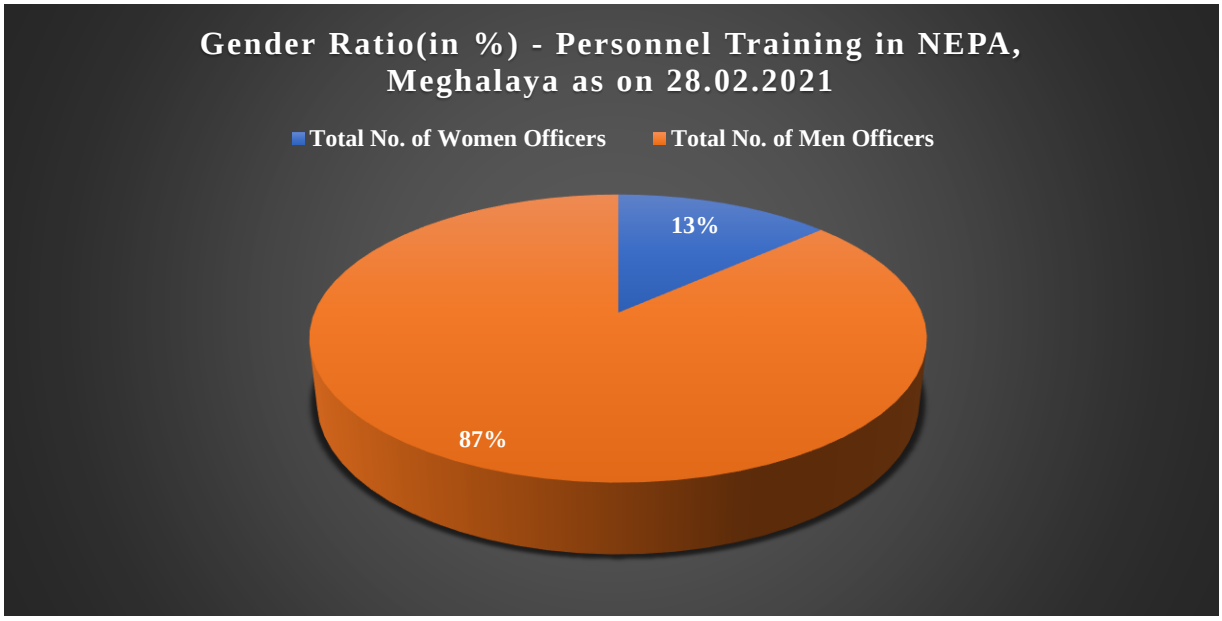
Graph 27 Gender Ratio in Personnel Training in States/UTs as on 28.02.2021



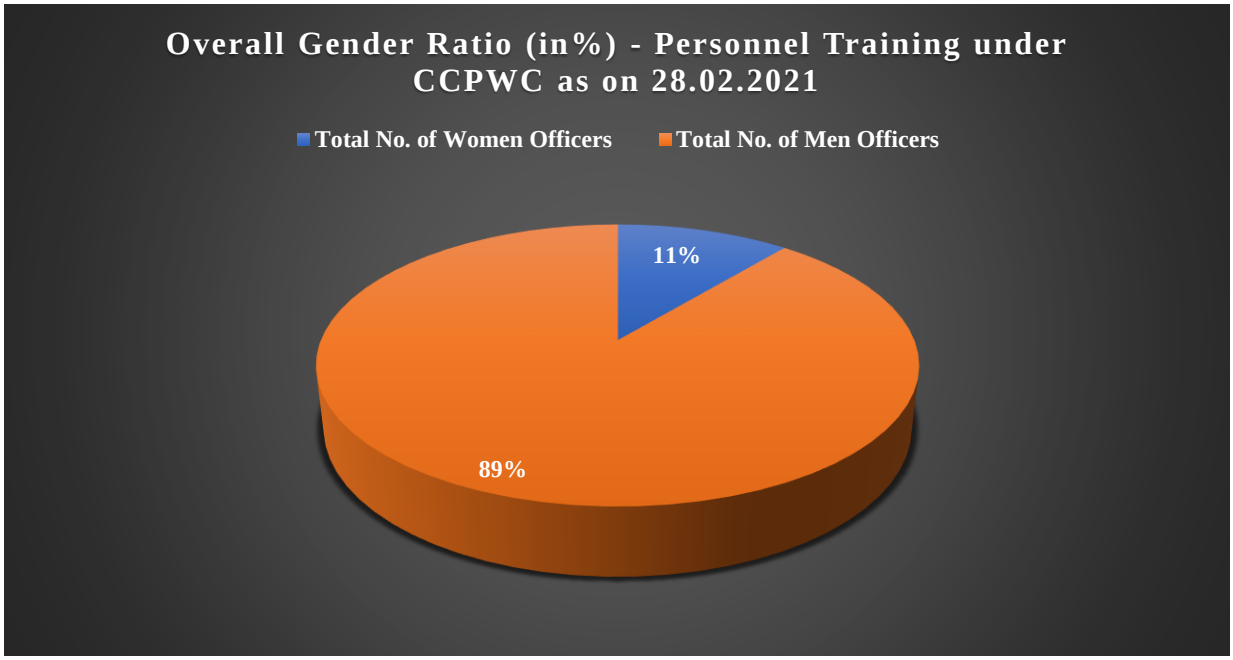
Graph 28 Gender Ratio in Personnel Training in SVPNPA, Hyderabad as on 28.02.2021

Graph 27 depicts the gender ratio percentages of the no. of women personnel trained as against the no. of men personnel in State/UTs. Women trainees comprised only about 11% of the total number of trainees for capacity building in States/UTs.

Graph 28 depicts the gender ratio percentage of the no. of women personnel trained as against the no. of men personnel in the training academy, SVPNPA Hyderabad. Out of the total strength, women trainees comprised about 12%.



Graph 29 Gender Ratio in Personnel Training in NEPA, Meghalaya as on 28.02.2021

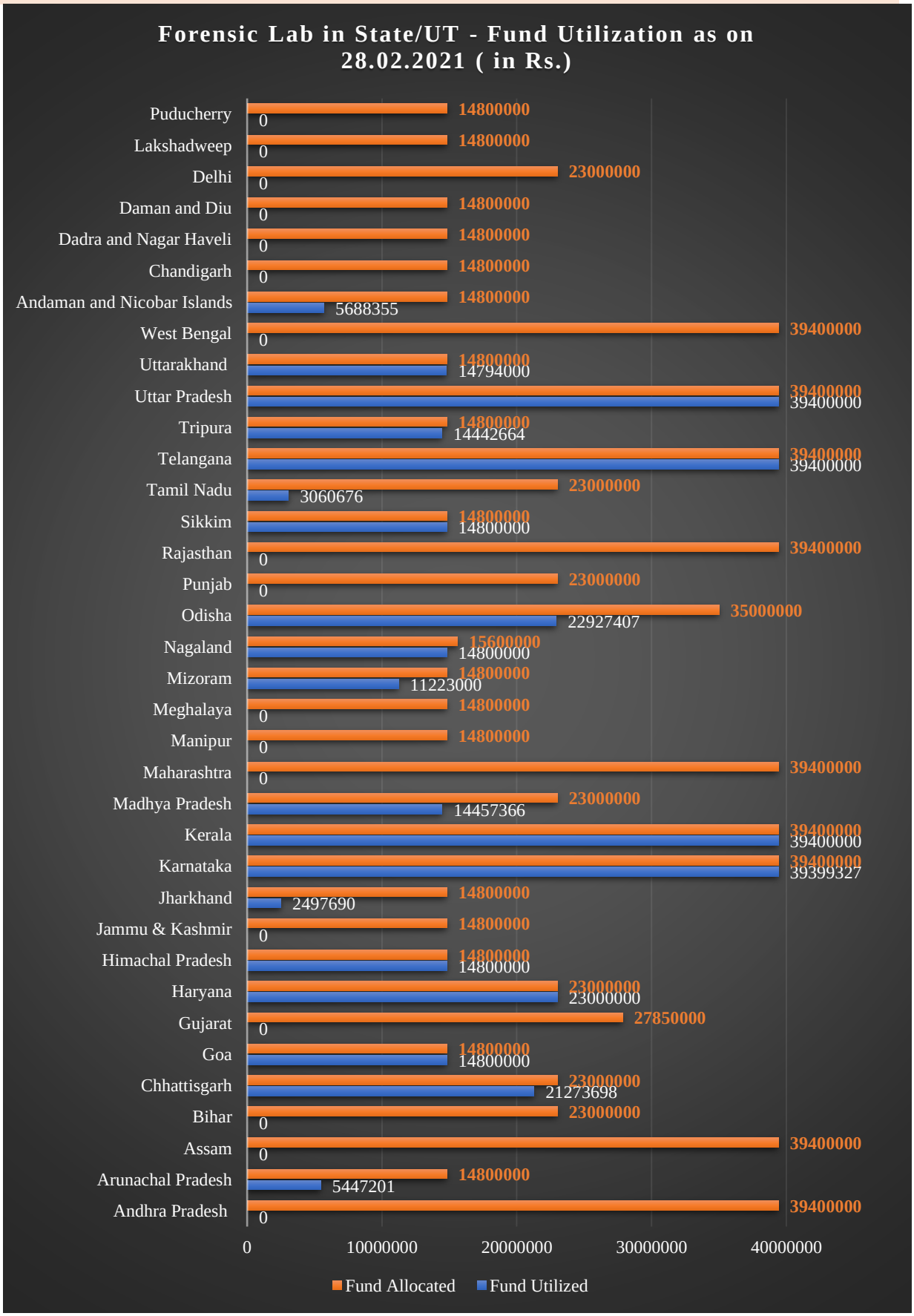


Graph 30 Overall Gender Ratio in Personnel Training under CCPWC as on 28.02.2021

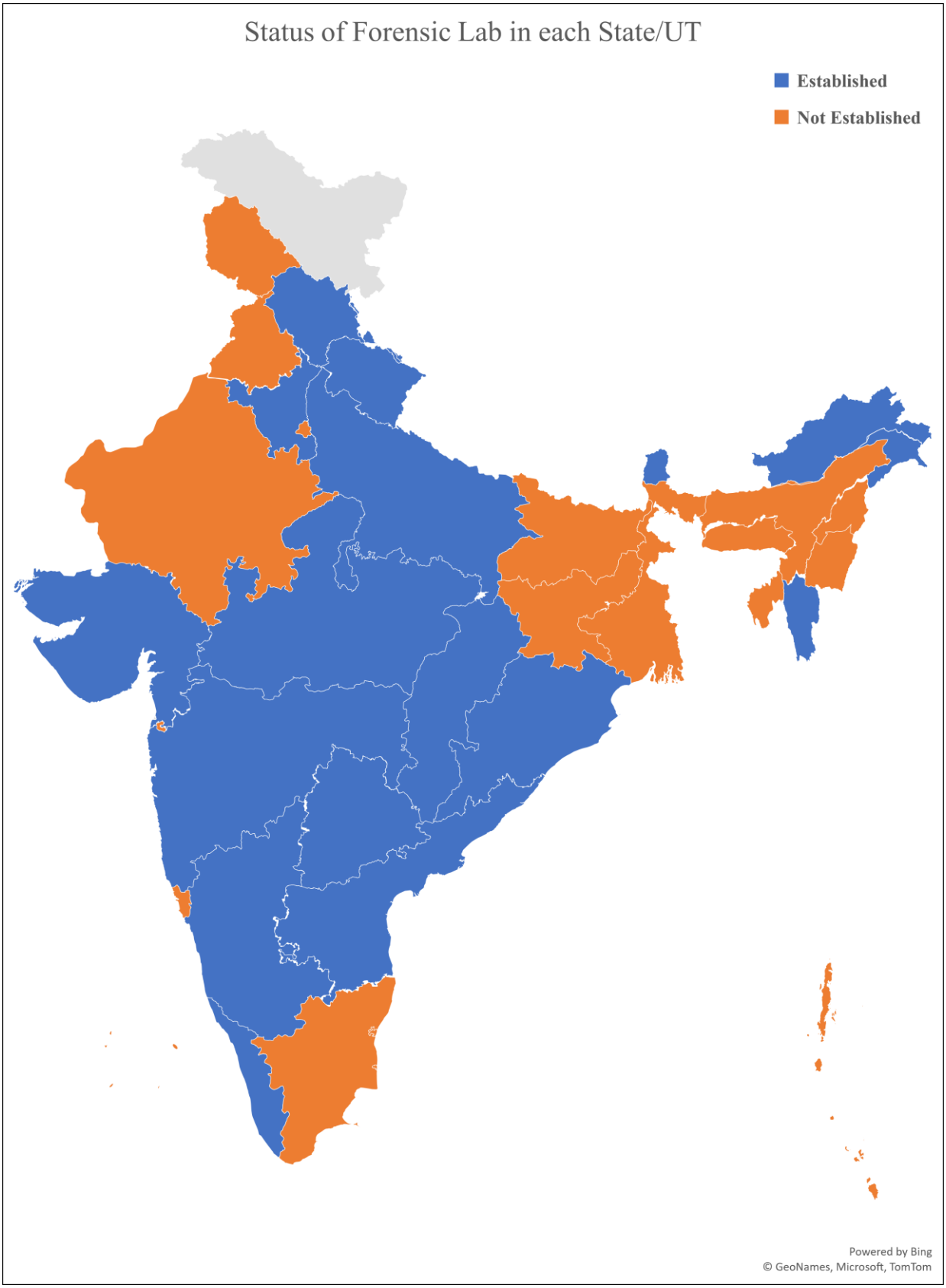
Graph 29 depicts the gender ratio percentage of the no. of women personnel trained as against the no. of men personnel in the training academy, NEPA Meghalaya. Out of the total strength, women trainees comprised about **13%**.

Graph 30 depicts the overall gender ratio of training being conducted under CCPWC. Women officials trained under CCPWC comprised about **11%** of the total number of personnel trained. Given that the scheme aims to enhance mechanism for women and children's cyber safety, this low gender ratio in personnel training needs to be improved.

IV. Capacity Building – Forensic Lab in each State/UT (Fund Allocation and Utilization)



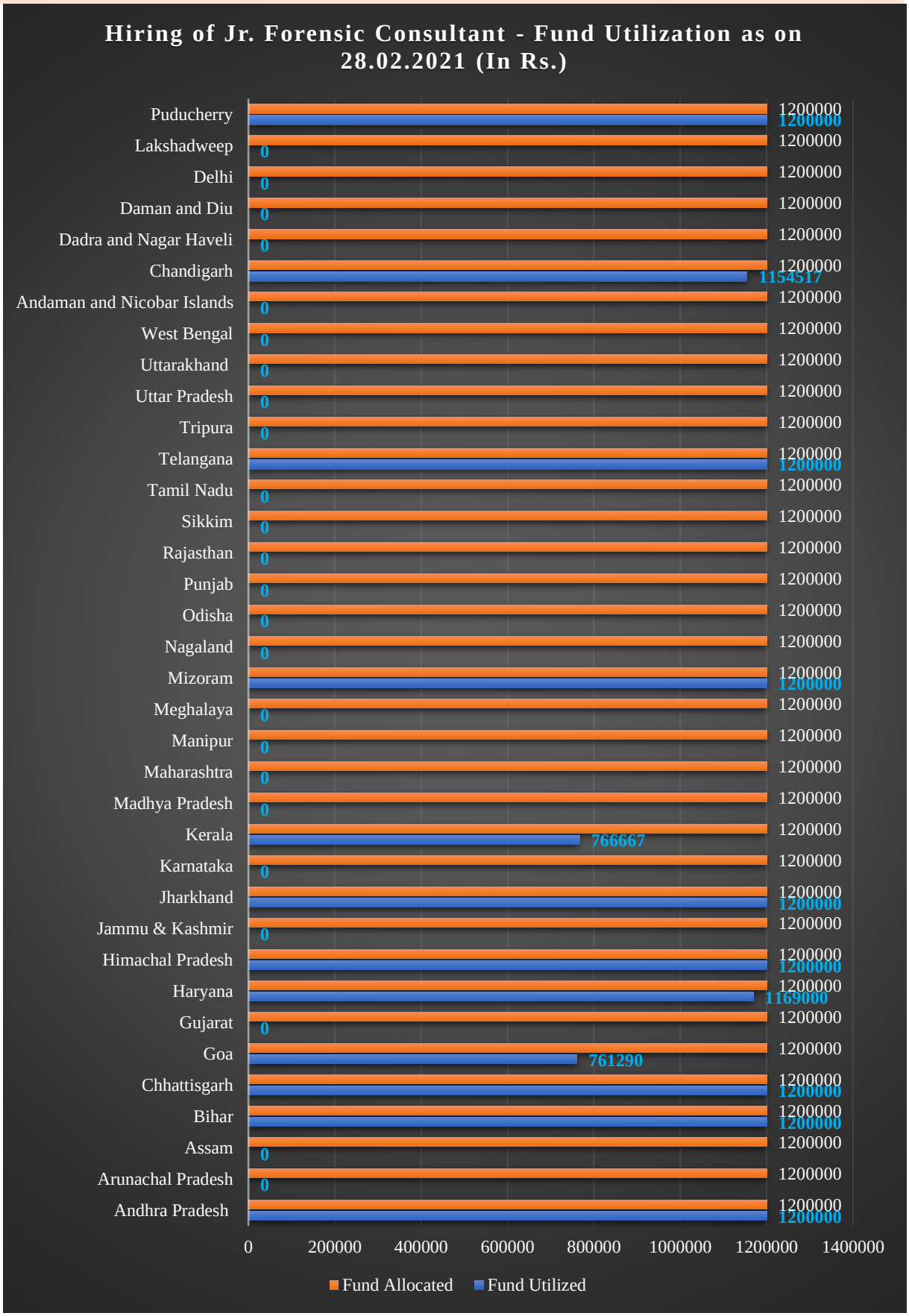
Graph 31 Forensic Lab in State/UT - Fund Utilization as on 28.02.2021



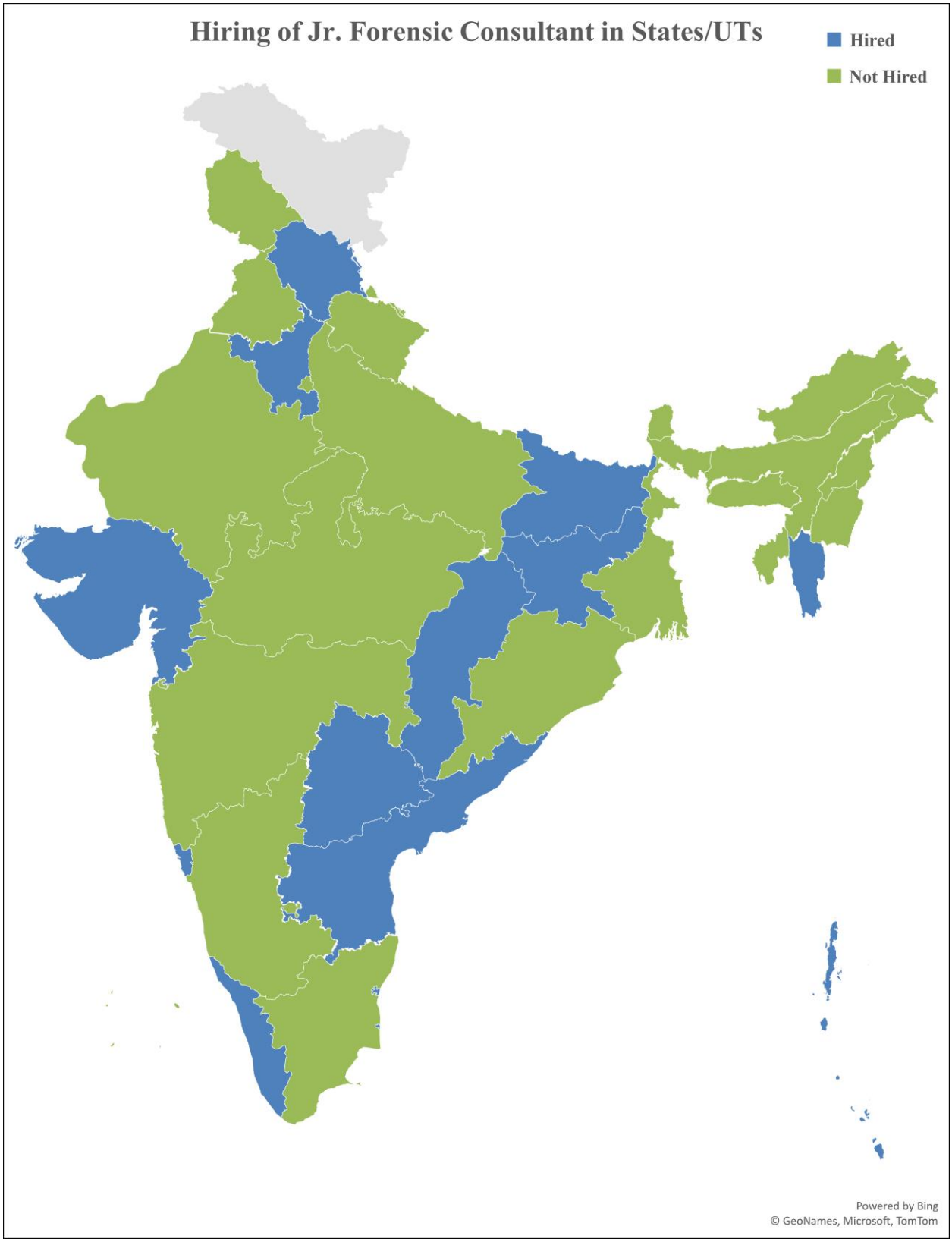
Graph 32 Status of Forensic Lab in States/UTs as on 28.02.2021

Graph 32 depicts the status of establishment of Labs in States/UTs. As on 28.02.2021, **17 States** have established Lab-cum-training facility while **19 States/UTs** have utilized their funds.

V. Capacity Building – Hiring of Jr. Forensic Consultant



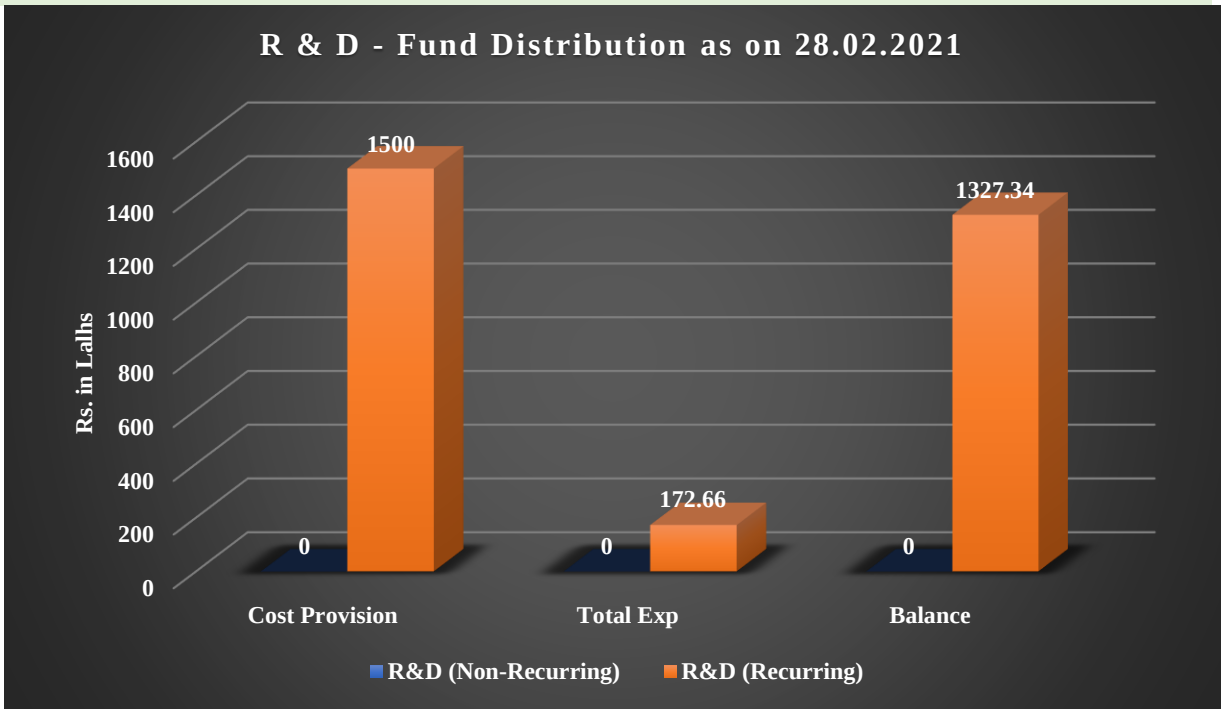
Graph 33 Hiring of Jr. Forensic Consultant - Fund Utilization as on 28.02.2021



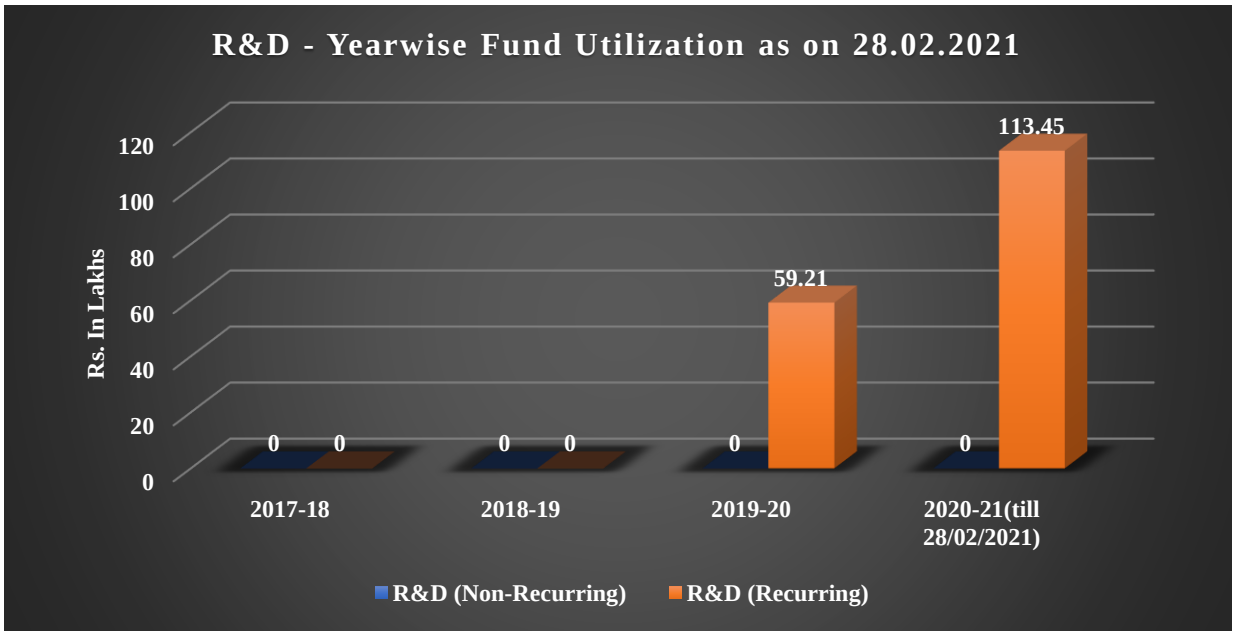
Graph 34 Hiring of Jr. Forensic Consultant in States/UTs

Graph 33 and **34** depicts the status of Hiring of Jr. Forensic Consultants in each State/UT. As on 28.02.2021, a total of **12 States/UTs** have utilized their funds while **14 States/UTs** have hired consultants.

3.2.4. Research & Development (R&D)



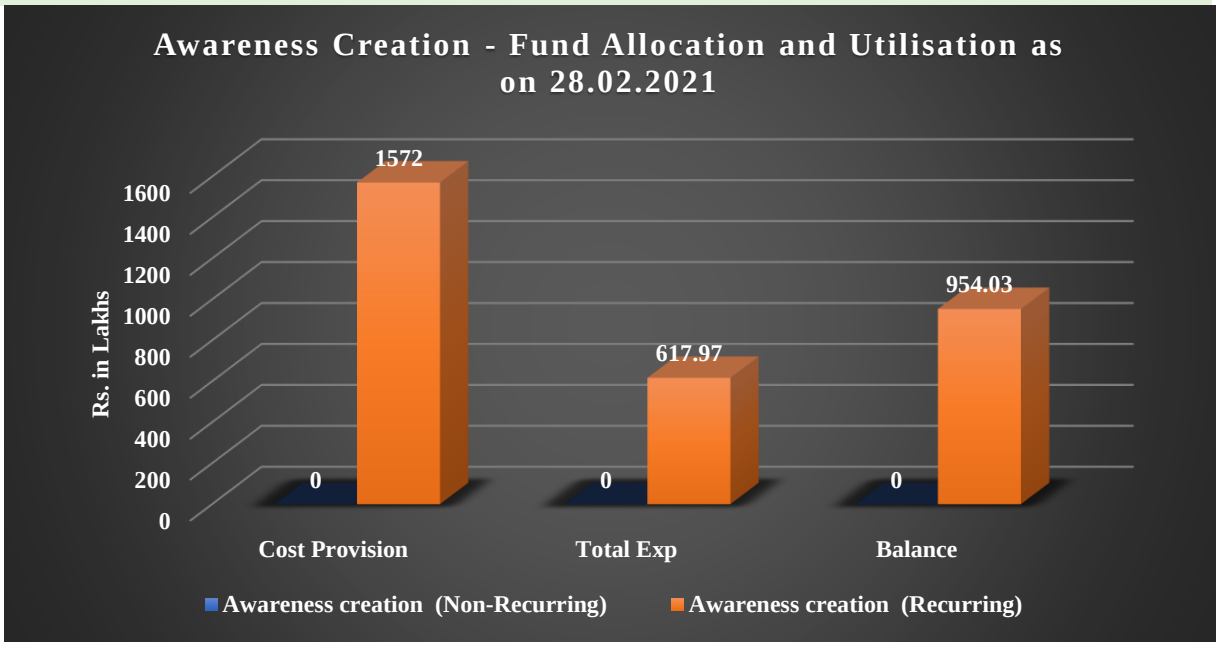
Graph 35 R & D - Fund Distribution as on 28.02.2021



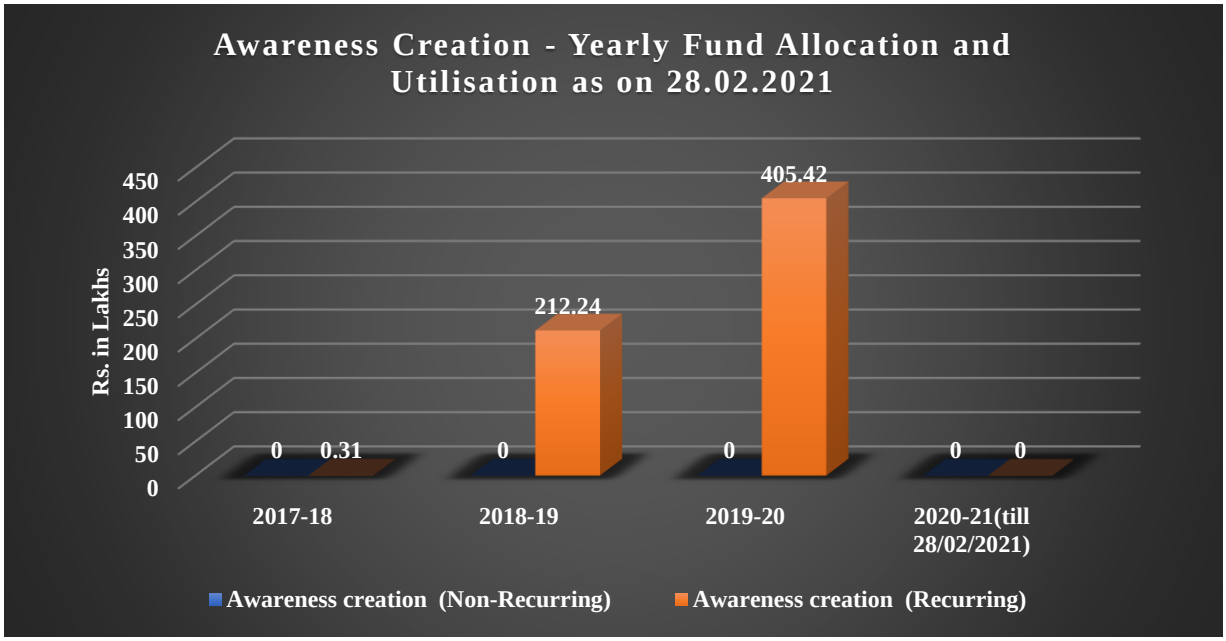
Graph 36 R & D - Year wise Fund Utilization as on 28.02.2021

Graph 35 and **36** depicts the overall and yearly fund allocation & utilization under Research & Development (R&D) component of the CCPWC Scheme. As on 28.02.2021, a recurring expenditure of **Rs. 172.66** lakhs have been incurred in carrying out the R&D projects. And, as on date, BPR&D, the implementing agency, has sanctioned a total of 9 projects. The total cost provision for this component under CCPWC is Rs. 1500 lakhs.

3.2.5. Awareness Creation

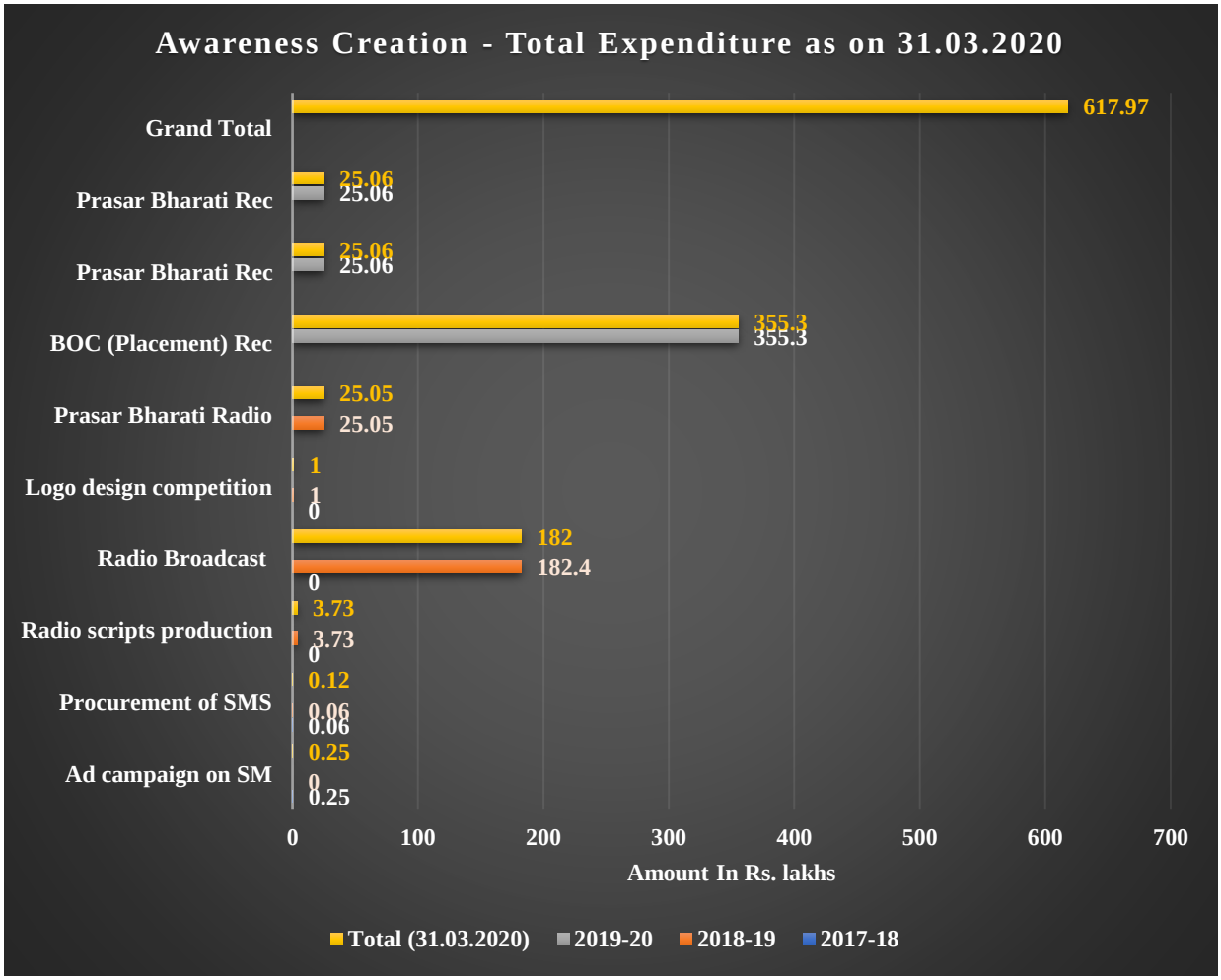


Graph 37 Awareness Creation - Fund Utilization as on 28.02.2021



Graph 38 Awareness Creation - Yearly Expenditure (2017-2021) as on 28.02.2021

Graph 37 and **38** depicts the overall and yearly fund allocation & utilisation under the Awareness Creation component of CCPWC Scheme. As on 28.02.2021, a total of Rs. 617.97 lakhs have been spent in spreading awareness against cybercrimes against women and children. The total cost provision for this component under CCPWC is Rs. 1572 lakhs. The expenditure details are further elaborated upon in **Graph 39** and **Table 17** on the next page.



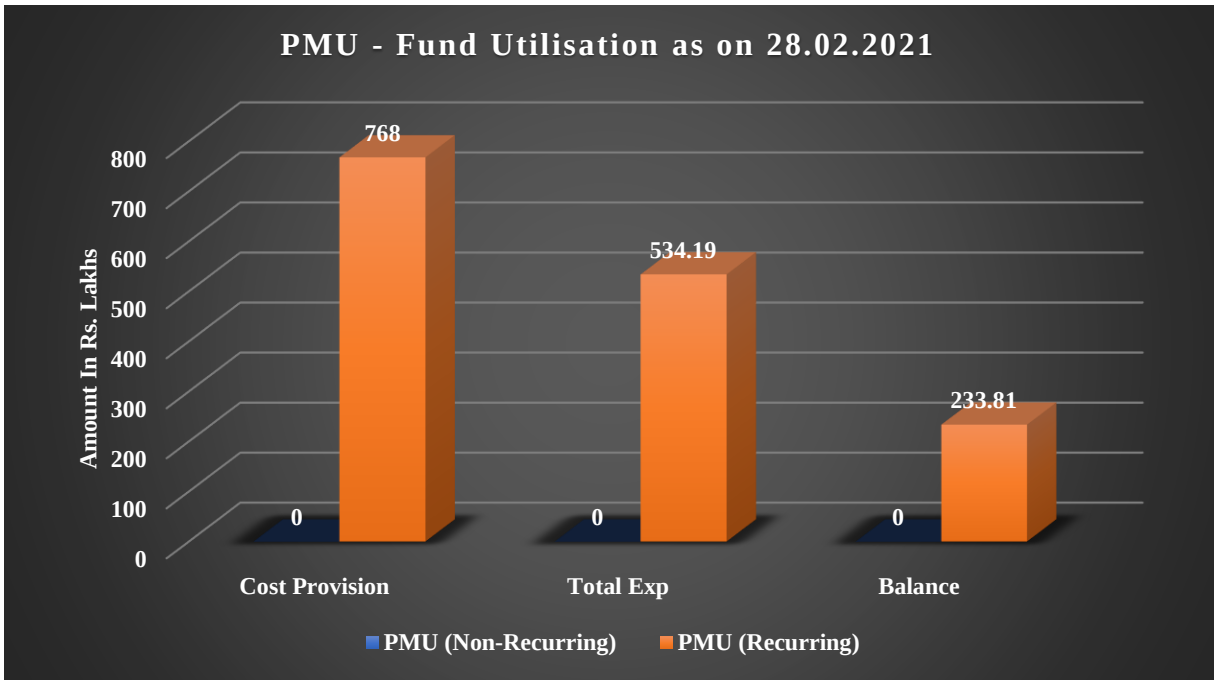
Graph 39 Awareness Creation - Total Expenditure as on 31.03.2020

Table 17 Awareness Creation expenditure under different Heads

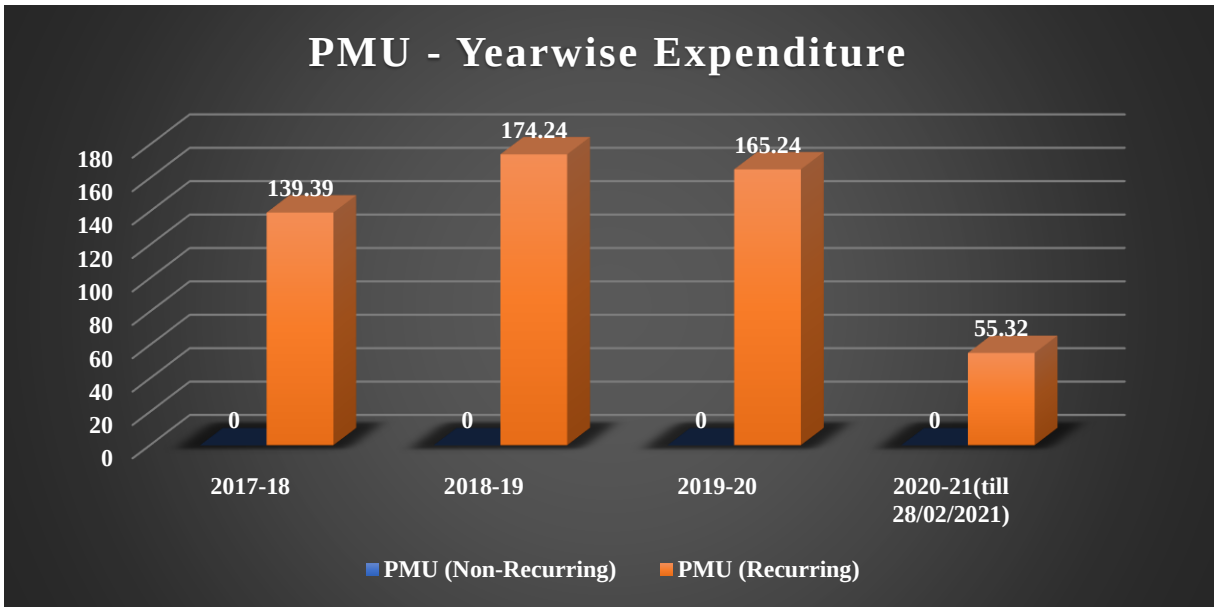
Awareness Creation - Expenditure	2017-18	2018-19	2019-20	Total
Ad campaign on SM	0.25	0		0.25
Procurement of SMS#	0.06	0.06		0.12
Radio scripts production	0	3.73		3.73
Radio Broadcast	0	182.4		182.4
Logo design competition	0	1		1
Prasar Bharati Radio		25.05		25.05
BOC (Placement) Rec			355.3	355.3
Prasar Bharati Rec			25.06	25.06
Prasar Bharati Rec			25.06	25.06
Grand Total (Rs. In Lakhs)				**617.97**

Procurement of 2+1.95 lakh SMSs in connection with operational OTP services for integration of online Cybercrime Reporting Portal with CCTNS

3.2.6. Project Management Unit (PMU)

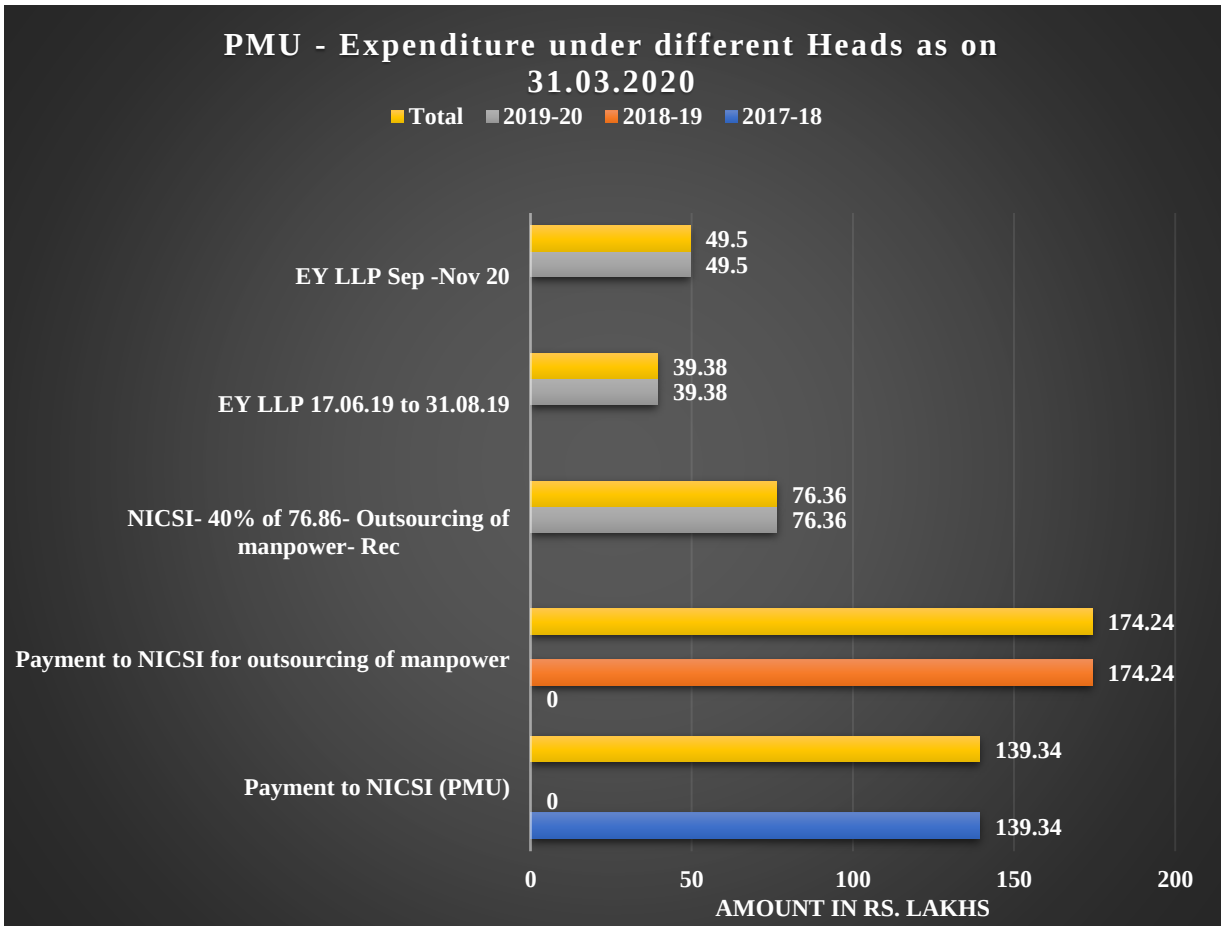


Graph 40 PMU - Fund Utilisation as on 28.02.2021



Graph 41 PMU - Year wise Expenditure as on 28.02.2021

Graph 40 and **41** depicts the overall and yearly fund allocation & utilisation under the PMU component of CCPWC Scheme. As on 28.02.2021, a total of Rs. 534.19 lakhs have been spent on operationalizing the component. The total cost provision for this component under CCPWC is Rs. 768 lakhs. The expenditure details are further elaborated upon in **Graph 42** and **Table 18** on the next page.



Graph 42 PMU - Expenditure under different Heads as on 31.03.2020

Table 18 Payment to NICSI is for hiring of personnel for setting up PMU

PMU - Expenditure Heads	2017-18	2018-19	2019-20	Total
Payment to NICSI (PMU)	139.34	0		**139.34**
Payment to NICSI for outsourcing of manpower	0	174.24		**174.24**
NICSI- 40% of 76.86- Outsourcing of manpower- Rec			76.36	**76.36**
EY LLP 17.06.19 to 31.08.19			39.38	**39.38**
EY LLP Sep -Nov 20			49.5	**49.5**
Grand Total				**478.82**

3.3. Salient Findings

1. As on 28.02.2021, under the CCPWC scheme, the total expenditure is Rs.11649.13 lakhs i.e., **52.20%** and the balance amount is Rs. 10670.67 lakhs i.e., **47.80%** of the total outlay. The total outlay under the scheme is Rs. 22319.8 lakhs.
2. Further, in 2017-18, the expenditure incurred was Rs. 8969.25 lakhs i.e., **76.99%** of the total expenditure; in 2018-19 it was Rs. 524.3 lakhs (**4.50%**); in 2019-20, the expenditure was Rs. 1768.48 lakhs (**15.18%**); and, in 2020-2021 till February 2021, the expenditure has been Rs. 387.1 lakhs (**3.32%**).
3. The component of online cybercrime reporting portal has been allocated a total of Rs. 3664.8 lakhs. However, the total expenditure incurred as on date has been only Rs. 296.86 lakhs i.e., **8.10 %** of the total allocated amount.
4. The total expenditure incurred under NCFL(E) component is Rs. 553.42 lakhs i.e., **14.82 %** of the total allocated amount i.e., Rs. 3734 lakhs. The expenditure pertains to procurement of hardware/software tools, hiring of **37** technical professionals for the Lab and other operational expenditure.
5. The total allocation to States/UTs is Rs. 9577.23 lakhs and the total utilization is Rs. 3883.46 lakhs i.e., **40.54 %** of the total allocated amount. The total expenditure pertaining to the three subcomponents is Rs. 8456.50 lakhs (**88.3%**) for establishing Forensic Lab in each State/UT, Rs. 688.73 lakhs (**7.19%**) for conducting trainings, and Rs. 432 lakhs (**4.33%**) for hiring Jr. Cyber Consultant.
6. Under different categories of States/UTs, the total allocated amount to Category A is Rs. 3978.32 lakhs (**41.54%**), to Category B is Rs. 2637.25 lakhs (**27.54%**) and to Category C is Rs. 2961.65 lakhs i.e., **30.92%** of the total allocated amount. The total allocated amount is Rs. 9577.23 lakhs.
7. As on 28.02.2021, of the 36 States/UTs, 33 States/UTs received funding. Out of the **33**, **14** States/UTs have utilized the funds for conducting trainings for LEAs.
8. The total number of Women personnel trained is **1319** while the total number of Men personnel trained is **10648**. The total number of Judicial officers trained is **762** while the total number of Public Prosecutors trained is **950**. The grand total no. of personnel trained is **13679**.
9. As on 28.02.2021, the women personnel trained under Capacity Building component of CCPWC comprised about **11%** of the total number of personnel trained.

10. As on 28.02.2021, **19** States/UTs have utilized their funds for establishing Forensic lab-cum-training facilities and **17** States have established Labs-cum-training facilities.
11. As on 28.02.2021, a total of **12** States/UTs have utilized their funds for hiring Jr. Cyber Forensic Consultant while **14** States/UTs have hired the consultants.
12. A recurring expenditure of Rs. 172.66 lakhs (i.e., **11.51%** of the total allocated amount) have been incurred under the R&D component. And BPR&D, the implementing agency, has sanctioned a total of 9 projects. The total cost provision for this component under CCPWC is Rs. 1500 lakhs.
13. A total of Rs. 617.92 lakhs (i.e., **39.31%** of the total allocated amount) have been spent in spreading awareness against cybercrimes against women and children under Awareness Creation component. The total cost provision for this component under CCPWC is Rs. 1572 lakhs.
14. A total of Rs. 534.19 lakhs (i.e., **69.55 %** of the total allocated amount) have been spent on operationalizing the PMU component. The total cost provision for this component under CCPWC is Rs. 768 lakhs.

3.4. Scheme Achievements

S. No.	Objectives of CCPWC Scheme	Achievement(s)
1.	Setting up of Online Cyber Crime Reporting Portal and related units	A Cybercrime Reporting Portal (www.cybercrime.gov.in)" was launched on 20th September 2018. The Portal provides a centralized platform to enable citizens to report online content pertaining to Child Pornography (CP)/ Child Sexual Abuse Material (CSAM) or sexually explicit content such as Rape/Gang Rape (CP/RGR). The revamped version of the National Cyber Crime Reporting Portal was launched (under I4C) on 30.08.2019 which enable citizens to report all kinds of cyber-crimes with special focus on cyber-crime against women and children.

		Over 3.00 lakh complaints have been registered on the portal as on 31.01.2021 and more than 5000 FIRs registered based on these complaints. Cyber-crime reporting portal launched on 20.09.2018 to provide a centralized platform to enable citizens to report online content pertaining to Child Pornography(CP)/Child Sexual Abuse Material (CSAM) or sexually explicit content such as Rape/Gang Rape (RGR). Revamped version of this Portal was launched on 30.08.2019, which allows reporting of all types of cyber-crimes with special focus on cyber-crimes against women and children. Incidents/complaints reported on this portal are routed automatically to the respective police authorities of States/UTs based on the information furnished by the complainants. The Portal facilitates the States/UTs to view complaints of cyber-crime online and take prompt action. National Crime Record Bureau (NCRB) has been notified as an agency of Government of India on 13.08.2018 to issue notices to intermediaries under section 79(3)(b) of the IT Act for removal of Child Pornography (CP), Rape & Gang Rape (RGR) content. NCRB has issued 14 notices to the intermediaries under section 79(3)(b) of the IT Act.
2.	Establishment of National Cyber Forensic Laboratory (Evidence purpose)	Directorate Forensic Science Services (DFSS) has been assigned to set up NCFL at Hyderabad for evidentiary purpose i.e., NCFL (E) with an outlay of Rs.37.34 Crores. Establishment of this laboratory will provide the necessary

		forensic support in cases of evidence related to cyber-crime, preserving the evidence and its analysis in line with the provisions of IT Act and Evidence Act; and will reduce turnaround time. This laboratory will act as a Model Laboratory for other Central and State Forensic Science Laboratories in the country. The Lab is expected to be made fully operational in March 2021. Civil work has been completed and major equipment have also been installed. Procurement of a few essential equipment & software are underway. This laboratory is expected to be made functional by the end of March 2021.Turnaround time to examine & submit the evidence will be reduced after its fully operationalisation.
3.	Capacity Building	Provided grants of Rs.95.77 crore to all the States and UTs under CCPWC scheme to setup cyber forensic cum training laboratories, training and hiring of junior cyber consultant so as to provide hands-on training to LEAs and Judiciary. Cyber forensic-cum training laboratories have been established in 17 States/UTs namely, Arunachal Pradesh, Andhra Pradesh, Chhattisgarh, Gujarat, Haryana, Himachal Pradesh, Karnataka, Kerala, Madhya Pradesh, Maharashtra, Mizoram, Odisha, Sikkim, Telangana, Uttarakhand, Uttar Pradesh, and Chandigarh. Prepared 3-day, 5-day and 10 days training programs for law enforcement agencies, public prosecutors, and judges for improving the conviction rate and cyber-crime awareness in cyber-crime cases, in consultation with the stakeholders and requested State Governments/Union Territories to organize training programs. So far, more than 13500 Police personnel, Judicial Officers and Public Prosecutors have been provided

		training on cyber-crime awareness, investigation, forensics, etc.
3.(a)	Establishment of Cyber Forensic-cum-Training Labs in each State/UT under Capacity Building (36 States/UTs)	17 States/UTs have commissioned Cyber Forensic-cum-Training Laboratories. Establishment of Cyber Forensic-cum-Training Laboratories in remaining 19 States/UTs is underway.
3.(b)	Hiring of Junior Cyber Consultants under Capacity Building (@Rs.12.00 lakh per annum to 36 States/UTs for a period of 3 years)	Financial support @Rs.12.00 lakh for one (first) year has been provided to each States/UTs for this purpose. So far 13 States/UTs have hired Jr. Cyber Consultants. Remaining States/UTs are at final stage of sourcing them out. As per the approval, the financial support@Rs.12.00 lakh per annum is to be provided to them for hiring of Jr. Cyber Consultants during remaining two years.
3.(c)	Training under Capacity Building (Targeted to train 40500 LEAs/PP/ Judicial Officers)	So far more than 13500 LEAs' Personnel/Judicial Officers/Public Prosecutors have been provided training on cyber-crime awareness to enhance their skills to investigate cyber-crimes, secure electronic evidence, conduct forensic analysis, produce the evidence in the court of law, etc. Remaining targets are required to be achieved.
4.	Research and Development	9 R&D projects in the field of cybercrimes approved by the Govt. Out of which 7 R&D projects sponsored to the Academic Institutions. Funds are being released to the selected Institutions as per conditions laid down in MoU signed between BPR&D and the Institute concerned. Remaining 2 projects are being sponsored to the concerned Institutions and the process of signing MoU is underway.

5.	Awareness Creation	Launched Radio campaign across the country by Ministry of Home Affairs for six months to spread awareness among the public against cyber-crimes. Information Security best practices booklet is also released for the benefit of Government Officials. Released an easy to understand 'Handbook for Adolescents/ Students' booklet for the age group of 13 years or more to enhance awareness about Cyber Crimes. Circulated this booklet to the Secretaries of all Ministries/Departments, Chief Secretaries of State Governments/UTs and DGsP, for wide spreading it to their respective areas and also made it online available at www.cybercrime.gov.in and https://mha.gov.in/documents/downloads.
6.	Project Management Unit (PMU)	Deployed a dedicated professional Project Management Unit (PMU) to ensure proper monitoring & implementation of all the initiatives under this scheme and to assist MHA as and when required.
7.	Engagement with National and International NGOs/ International bodies	Memorandum of Understanding (MoU) has been signed between the National Crime Records Bureau (NCRB), India and the National Centre for Missing and Exploited Children (NCMEC), USA regarding receiving of Tip line report on online child pornography and child sexual exploitation contents from NCMEC. A total of 3.83 lakhs Cyber Tip line reports have been shared with concerned States/UTs till 31.01.2021 by NCRB in the form of CDs/DVDs. More than 600 FIRs have been registered based on the Tip line.

		NCRB has planned to integrate NCMEC Cyber Tipline in the Cybercrime Reporting Portal. Thereafter, the Tipline will be routed automatically to States/UTs for taking further steps.
8.	Legal regulations	An SOP for examining the complaints and issue of notice has been formulated and circulated to LEAs of all States/UTs. Ministry of Home Affairs has shared the recommendations with MeitY for amendments in the provisions of Information Technology Act, 2000 and Information Technology (Intermediary Guidelines) Rules, 2011.
9.	Creation of Hash Bank	The facility for creation of Hash Bank is covered in the proposal submitted by C-DAC for setting up of Pro-active Monitoring facility. Proposal submitted by NCRB in consultation with C-DAC Mumbai, for setting up of Pro-active Monitoring facility has been approved for execution.
10.	Setting up of content monitoring and analysis unit	
11.	Setting up hotline for reporting of cybercrime related to Women & Children	A toll-free help line number 155260 has been launched by the central government to help the person, if problem comes in reporting the incident/complaint online, in their own languages. The services of this helpline functions in decentralised manner and the calls received on this number is attended & responded by the call centre executive of the respective States/UTs.
12.	Setting up of a keyword repository in coordination with stakeholders	List of keywords with the help of stakeholders (in English-505, Hindi-87, Bengali-15, and Kannada-22) were compiled by MHA and conveyed to prominent Search Engines for taking further necessary action in the matter. Facility has been provided on National Cyber Crime Reporting Portal for public to anonymously report keywords which lead to CSAM/RGR content when searched in Search Engines.

13.	Dedicated national agency for coordinating cybercrime prevention, detection and supporting investigations	While appraising the CCPWC Scheme in 2018, it was indicated that the activities of CCPWC would be monitored and administrated by the proposed Indian Cyber Crime Coordination Centre (I4C) and would coordinate with States/UTs for implementation of all components of the scheme. I4C has been set up in Ministry of Home Affairs at New Delhi. While reviewing the physical & financial progress of CCPWC Scheme, the Empowered Committee, in its meeting held on 01.02.2021, had recommended for extension of implementation period of the scheme by two years without additional fund allocation, to facilitate completion of assigned pending activities by its stakeholders.

CHAPTER 4 :

SUGGESTIONS AND RECOMMENDATIONS

4. SUGGESTIONS AND RECOMMENDATIONS

In the last decade, India has seen a rapid rise in the cybercrime cases happening against women and children. The increasing number of cases have drastically victimised large number of young working women and young students in the country. There are numerous ways in which the cyber criminals attack and trap their victims by, e.g., Cyber stalking, Cyber bullying, Cyber harassment, Identity theft, Breach and violation of privacy/confidentiality, Voyeurism, pornography, Email spoofing, morphing of images for pornographic content, and Dark Web etc. Moreover, the nature of cybercrimes is based on a virtual reality which has no limitations when it comes to national or international physical boundaries. Therefore, cybercrimes not only endanger victims' lives but also create a menace for the LEAs in resolving the cases.

However, the global community is now rising to this challenge and now cyber security has become one of the most important topics of discussions on world forums. The policies on cybercrimes have taken a centre stage in almost all political discussions. In India too, the government's emphasis on Digital India has given a push to development of cyber safeguards as well. The CCPWC scheme of Government of India is indeed a vital step in this direction. The scheme aims to establish an effective mechanism to handle cybercrimes against women and children in the country.

In this regard, the scheme comprises of six components, namely, online cybercrime reporting portal, one national level cyber forensic lab, capacity building in States/UTs, Awareness Creation, Research & Development, and Project Management Unit. The scheme and its subcomponents aim to create a network of interstate capabilities in effectively handling cybercrime investigations. Each sub-component of the scheme covers different aspect of handling cybercrimes in a strategic manner so that coordination between all the agencies and LEAs may function in a smooth and faster way.

During the process of evaluation, the IIPA study team analysed all the scheme related documents and data in terms of implementing mechanism, fund allocation and utilization, present status, scheme achievements and issues or challenges. Based on the analysis and observations, the study team found that the scheme, since its inception in 2017, has been able to perform satisfactorily under all its subcomponents, specifically, Online cybercrime reporting portal by NCRB, Capacity Building in States/UTs, establishment of NCFL(E) at CFSL in Hyderabad, Awareness Creation activities via radio broadcasts, publications and social media

platforms and sanctioning of R&D projects by BPR&D. Despite the limitations faced due to Covid-19 Pandemic, the trajectory of the scheme's performance further reflects that with the adequate financial and implementation support, the scheme will successfully achieve its desired objectives.

Based on the observations made during its evaluation, IIPA study team also highly recommends the continuation of the scheme. The study team would also like to share a list of certain suggestions and recommendations for further enhancement of the scheme.

The suggestions and recommendations are as follows:

1. **Emphasis on Fund Utilization**

   The CCPWC scheme is successfully moving towards achieving it set targets as many of its components have been able to begin functioning and utilize the funds allocated to them. Given the limitations that were posed in last two years due to the Covid-19 pandemic, the progress on the scheme performance is showing satisfactory trends. It is, however, suggested that more focus be laid on the States/UTs still struggling with their fund utilization. Other States/UTs and stakeholders who have been able to utilise their funds may also continue to be encouraged and supported with sufficient fund allocation for the future activities.

2. **Increase Manpower**

   One of the major problems faced by LEAs in cybercrime investigations is the lack of skilled and technical manpower. Investigation of cybercrime requires a set of investigative skills and technical knowledge in analysis and tracking of leads/trails. Therefore, it is emphasised to increase manpower enhanced by conducting trainings, be available in all States/UTs for handling cybercrimes against women and children.

3. **Procurement of Advanced Tools and Technology**

   Most of the cybercrime cases face difficulty in getting solved due to lack of essential equipment and manpower. Therefore, along with manpower, investigation of cybercrimes also requires availability of latest tools and technology for the LEAs to solve cybercrimes. Under the scheme, many states have been able to establish cyber forensic lab-cum-training facility and hire a consultant but there is still a lack of advanced tools for their effective

functioning. It is, hence, suggested that states/UTs which have been able to utilise funds in this direction may be now encouraged and supported for adequate procurement of required equipment(s).

4. **SOPs to be followed by all States/UTs LEAs**

While the current portal enables the victim/ complainant to lodge grievances it does not offer any feature for law enforcement agencies to avoid duplication in effort if the same content is reported from another state/ UT. Also, many states still do not follow SOPs which cause unnecessary delays and hamper the effectiveness of LEAs. It is therefore suggested that focus on development of standardised SOPs and their strict enforcement by all LEAs may be made an essential part of the scheme.

5. **Development of a Mobile Application for Effective Reporting**

Since we are living in a digital age and mobile phones have become an inevitable part of our lives, especially becoming popular among the teenage and adolescent age groups, CCPWC scheme could also focus on developing a mobile application based on Android or iOS which is user-friendly and ensure user privacy. The App may also function as an Awareness creation tool by incorporating interactive infographics and videos for its end users.

6. **Monitoring and Evaluation of Cybercrime Landscapes**

Since the virtual world keep evolving every day and the face of cyber threats keep changing, social media and other online content hosting platforms need to be closely monitored for strict compliance to national cyber laws of the country. In this regard, it is suggested that a team of cyber experts may be present in all States/UTs as well as on a national level for ensuring proactive monitoring and evaluation of changing trends of cybercrimes. Regular meetings of these teams may take place for timely analysis of cybercrimes happening across the country.

7. **Interactive Sessions with School and College Students**

During the Covid-19 pandemic, online education emerged as the saviour of the day for millions of students across the country. This led to a rise in use of Mobiles, Tablets, and laptops by the young students. During the same time, the reports of cyber frauds and harassment faced by these young students as well as their parents also started emerging.

Therefore, it is suggested that school and college level interactive sessions in the form of debate competitions, Hackathons, theatre activities and painting competitions etc. may be organized under the Awareness Creation component of CCPWC scheme.

8. **Access to storage on Cloud space for quicker resolvement of cybercrime cases**

At present, the integrated network of online reporting portal and CCTNS with State portals face difficulties in timely redressals of cases due to a lack of access to storage on cloud space. The LEAs have to go through a time taking process of uploading and downloading large files related to the cases every time they need access to any case. Therefore, it is suggested to lay emphasis on procuring a virtual storage on cloud space and interlink it all the different portals.

9. **Harnessing Predictive Analytics Technique in Cyber Security**

Cyber security requires an ever more proactive approach, and the historical and real time data need to be analysed to identify patterns and detect anomalies in real time basis. Therefore, it is emphasised to employ innovative and sophisticated techniques like predictive analytics in ensuring cyber security. Predictive analytics uses self-learning analysis and detection techniques to monitor network activity and report real-time data breaches as well as identify the likelihood of future outcomes based on the past data.

10. **Integration of e-Court Services for Cybercrime Cases**

In the cybercrime reporting portal, there is already a provision for repository of court cases related to cybercrime cases and judgments. It is, therefore, emphasised that CCPWC scheme may ensure faster integration of e-Court Services with the platform to aid in faster resolvement of the registered cybercrime cases. The judgements of the same cases, then, may also be used as references in future judicial proceedings. Furthermore, integration of e-court services will clear the pre-existing log of cases and bolster the process of proactive identification of cyber threats and organized criminal groups for future readiness.

11. **Involvement of NGOs and Civil Society Groups in Cyber Safety Programmes**

To strengthen the cyber ecosystem at large it is suggested to increase the involvement of NGOs and other Civil Society groups by organizing programmes on cyber awareness and security specific to women and children's issues. Emphasis may be put on women participation. As observed during the study, rape threats, women safety and child

pornography have been among the major concern areas, this is also evident on NCRP platform wherein most complaints have been received related to these issues' category.

12. Capacity Building and Awareness creation in Semi-urban and Rural Areas

To spread awareness among the semi-urban and rural area populations, broadcasting may be carried out in local dialects with the help of All India Radio (AIR) and Doordarshan channel (DD). Informative videos or documentaries may be aired on local TV channels to increase the reach. Capacity building in these areas may also be aimed at empowering working women groups like SHGs, and other organizations.

13. Engagement with national and international NGOs/ International bodies:

Exchange program between private/ public bodies, NGOs and international bodies may be explored to establish effective utilization of expertise and enhancement of capabilities.

BIBLIOGRAPHY

https://www.mha.gov.in/

https://cybercrime.gov.in/

http://www.nepa.gov.in/

https://www.svpnpa.gov.in/

https://bprd.nic.in/

https://twitter.com/Cyberdost

https://ncrb.gov.in/

https://cfslhyd.gov.in/

https://indianexpress.com/article/india/wcd-announces-portal-to-tackle-cyber-crime-harassment-directed-against-women-children-ccpwc-4832580/

https://lawrato.com/legal-news/2494/victims-of-sexual-abuse-can-complaint-online-through-ccpwc-portal

https://rajeev.in/?questionasked=implementation-of-ccpwc-scheme

https://commons.wikimedia.org/wiki/File:The_Union_Home_Minister,_Shri_Rajnath_Singh_launching_the_Cyber_Crime_Prevention_against_Women_and_Children_(CCPWC)_portal,_in_New_Delhi.JPG

https://sarkariyojana.com/cyber-crime-prevention-women-children-ccpwc-portal/

https://morungexpress.com/nagaland-police-launches-ccpwc-lab-cum-training-center

https://www.ardcindia.org/scope/

https://timesofindia.indiatimes.com/city/goa/lack-of-equipment-staff-leave-80-cybercrimes-unsolved/articleshow/68193826.cms

https://www.dinalipi.com/odisha-police-to-be-trained-to-tackle-cyber-crimes-dgp/

https://www.mha.gov.in/sites/default/files/WSDivision_SheRakshaVol2_08112019pdf.pdf

https://www.businesstoday.in/technology/internet/cyber-dost-this-twitter-handle-tells-you-how-to-keep-your-online-personal-financial-data-safe/story/311678.html

https://www.mha.gov.in/sites/default/files/WSDivision_SheRakshaVol2_08112019pdf.pdf

ANNEXURES

ANNEXURE I

IIPA Questionnaire

for

Third Party Evaluation of Cyber Crime Prevention Against Women and Children (CCPWC) Scheme

Date: March 16, 2021

CCPWC Scheme component : **Development and Maintenance of Online Cybercrime Reporting Portal**

Implementing Agency : **NCRB**, Mahipalpur, NH-8, New Delhi

Please share the following details:

1. Fund Allocation and utilization under the CCPWC Scheme in the period (2017-2021)
2. Details of all the activities undertaken in development and maintenance of the online portal.
3. Details about the features and important aspects of the online portal.
4. How does the Portal support LEAs in achieving the scheme objectives i.e., to prevent cybercrime against women and child? What is the role of portal in investigation process and proceedings? Explain.
5. Details about the categories of cybercrime updated on the portal. Specify.
6. Any Issues and challenges faced during implementation or fund utilization? Specify.
7. What are the activities earmarked for the future?
8. Please provide your suggestions and recommendations regarding further improvement of the CCPWC Scheme.

ANNEXURE II

IIPA Questionnaire

for

Third Party Evaluation of Cyber Crime Prevention Against Women and Children (CCPWC) Scheme

Date: March 16, 2021

CCPWC Scheme Component : **Setting up of a State-of-the-Art Forensic Laboratory at CFSL, Hyderabad**

Implementing Agency : **DFSS**, CGO Complex, New Delhi

Please share the following details:

1. Fund Allocation and utilization under the CCPWC Scheme in the period (2017-2021)
2. Details of all the activities undertaken in setting up the Lab at CFSL, Hyderabad
3. What all challenges were faced during the set-up? Explain.
4. Details about the equipment(s) procured for the lab. Specify.
5. Status of the Lab, whether operational or not?
6. Details about the cases handled in the lab.
7. Details about all forensic/ investigative activities undertaken at the lab till date.
8. Highlight all the aspects of the Lab and its role in helping the LEAs.
9. Any Issues and challenges faced during implementation or fund utilization? Specify.
10. What are the activities earmarked for the future?
11. Please provide your suggestions and recommendations regarding further improvement of the CCPWC Scheme.

ANNEXURE III

IIPA Questionnaire

for

Third Party Evaluation of Cyber Crime Prevention Against Women and Children (CCPWC) Scheme

Date: March 16, 2021

CCPWC Scheme Component : **Research & Development**

Implementing Agency : **BPR&D**, NH-8, Mahipalpur, New Delhi

Please share the following details:

1. Fund Allocation and utilization under the CCPWC Scheme in the period (2017-2021).
2. Details about all the R&D projects undertaken till date.
3. Details of any national and international collaborations or joint projects undertaken.
4. Any Issues and challenges faced during implementation or fund utilization? Specify.
5. What are the activities earmarked for the future? Specify.
6. Please provide your suggestions and recommendations regarding further improvement of the CCPWC Scheme.