Cyber Crime Prevention against Women and Children(CCPWC)

August 30, 2019
***Source**: Press Information Bureau*

Objective

To have an effective mechanism to handle cyber crimes against women and children in the country.

Main components of the scheme are:

1.Online Cyber crime reporting Unit

- The "Online Cybercrime Reporting Portal" is a central citizen portal of the CCTNS project.
- Using this portal, an **online cyber-crime complaint** can be made by the victims of cyber-crime.
- It will provide a **central repository for all such crimes,** which will be used for publishing an annual analytical report regarding cyber-crimes, their trends and remedial measures etc.
- Also, this unit will provide a **central repository for reference to law enforcement and regulatory agencies** at the national, state and local level for cyber-crime related information.
- This unit will be responsible for the **development of an online cyber-crime reporting platform, publishing periodic analytical reports** covering trends of cyber-crime, defining process flows for handling online complaints field by citizens and also responsible for assigning such complaints to the appropriate law enforcement agencies based on jurisdiction in the states/ UTs or to any central agency having jurisdiction

for criminal investigation.

- This unit will work closely with forensic unit for all digital investigations at centre as well as at designated state forensic laboratories.

2.Forensic Unit

- **Proper collection and preservation of evidence related to cyber-**crime and its analysis in line with the provisions of the IT Act and evidence Act is of utmost importance.
- A national cyber forensic laboratory will operate 24*7*365 basis. It would have all the latest forensic tool setup, which would be accessible to all central /state/ UTs as well as central/ State forensic laboratories as and when needed.
- This unit will have a team of **cyber security professionals** to carry out vivid types of electronics forensic analysis and assist the law enforcement agencies in electronic forensic analysis across the country.
- This laboratory would carry all deep and advanced level forensic analysis.

3.Capacity Building Unit

- This unit will support **capacity building of Central and State Police Forces, Prosecutors, Judicial officers** and all other concerned stakeholder for all required capabilities like detection, investigations, forensic etc.
- This unit will also **assist the state/ UTs officials** in taking up long term courses to enhance the expertise in this area.

4.Research & development Unit

- In order to develop effective tools to detect obscene and objectionable content in the cyber space, a

continuous refining is needed. Hence, there is a need to take up research and development activities in partnership with research and academic institutions of national importance.

- These initiatives will help in improving the technology readiness and would be prepared to face any type of cyber-crimes. As part of research and development activities multiple Centres of Excellence (COE) will be developed in the country.

5.Awareness Creation Unit

- There is a need for a well-defined citizen awareness program by the government of India aimed at delivering cyber-crime dos and don’ts as a proactive mitigation initiative.
- Awareness about cybercrime and cyber hygiene will be introduced in schools in the early stages of education as a component of school curriculum.
- These awareness communications will be delivered via a web portal and mobile apps. Through this medium individual will be informed about the various types of cyber-crimes and information on how to securely use technology to protect themselves.
- **Awareness campaigns** like one day workshop, essay and elocution competition etc. will be conducted at schools, college level across the country and as a part of such programs brochures related to cyber etiquettes, do’s and don’ts and prizes would be distributed.