F.No 24013/31/2015-CSR-IV/CIS
Government of India/Bharat Sarkar
Ministry of Home Affairs/Grih Mantralaya

North Block, New Delhi-110001
Dated the 13th January, 2018

To

The Chief Secretaries of all State Governments/UTs Administrations

Subject: Advisory on Cyber Crime prevention and control

Over a period of time there has been phenomenal increase in use of computers, smartphones and internet. With this increase, cybercrimes have emerged as a major challenge for law enforcement agencies. Cybercrime cases are of varied types ranging from defacement of Government websites, online financial frauds, online stalking / harassment, Domain theft / Data theft etc. and each requires specialized investigative skill sets and forensic tools. Cybercrime cases pose technical, administrative as well as legal challenges in investigation. There is need to gear up institutional mechanism to tackle the cybercrimes and hence the following measures are suggested:

2. **Institutional setup:**

It is desirable to setup institutional arrangement for handling cybercrime at State & District level as proposed below:

i) **State Cyber Crime Coordination Cell:** Each State/UT may setup such units, preferably headed by a senior officer of ADGP/IG rank, designated as State Cyber Crime Coordinator. This cell may be responsible for setting up of institutional mechanism for handling cybercrime at District/police station level, guide & facilitate officers of such units, oversee capacity building, provide necessary lab resources, also take up investigation of specific cyber crime cases and coordinate with the State Cyber Crime Coordinators of other States in case of offences under IT Act, 2000 that fall under the jurisdiction of two or more States. Suitable number of police officers of various ranks and domain experts in the field of cyber security hired from the market should be part of such cell.

ii) **District Cyber Crime Cells:** The District Cyber Crime Cells may also be setup as per need, headed by Deputy Superintendent of Police / Addl SP supported by Sub Inspector / Inspector as deemed necessary and at least three domain experts in information technology, mobile telephony, digital forensics, cyber law hired from the market. Head of District Cyber Crime Cell may report to the District SP but seek overall guidance from State Cyber Crime Coordinator Cell of the State.

3. **Cybercrime cases involving Inter-State or international cooperation:**

Cybercrimes are borderless Crimes and may involve cooperation with other States or Countries. Hence it is important to strengthen inter-state and international cooperation mechanism. Following measures may be taken in this regard:

i) States may refer the specific cases which have inter-state or international ramifications to CBI which is also the nodal point for Interpol in India and executes LRs/MLATs.

ii) Strengthen inter-state coordination through joint investigation teams, evidence sharing and sharing of other information as appropriate for speedy disposal of cyber crime cases having inter-state ramifications.

4. **Cyber forensic labs:**

Most of the crimes committed, even in physical world use mobile as well as computer / internet in some form. Hence it is essential that adequate cyber forensic facility is created at State / District levels for investigating such cases. Following steps may be taken by the States / UTs in this regard:

i) MHA has released Rs 82.8 crore to States/UTs under CCPWC scheme for setting up a cyber forensic training lab cum training centre in each State/UT for their officials. All States/UTs must expedite setting up of this facility.

ii) States/UTs may consider setting up of cloud based high tech cyber forensic labs for efficient utilization of costly resources.

iii) Basic cyber forensic labs may be setup at District level as per need.

iv) Mobile cyber forensic lab facility may be explored for wider reach & optimal use of resources.

5. **Capacity building:**

Proper investigation and prosecution of cybercrime cases as well as assistance to the victims of cybercrimes require specialized knowledge and appropriate training of police officers, public prosecutors as well as judicial officers. Following measures may be taken proactively in this direction:

i) All police officers must be trained in basic cyber awareness.

ii) Sufficient number of officers must be trained in cybercrime investigations, forensic analysis and legal aspects as per need. Help of private institutes/experts may be taken as per need.

iii) BPR&D has made available lot of knowledge resources on its website and also provided 'E-Ustaad' e-learning platform for LEAs. UNODC also makes available free e-learning courses at https://golearn.unodc.org/lms/login/index.php. States/UTs are requested to encourage their police officers to train for use of for such resources.

iv) LEA officers working in cyber cells are encouraged to obtain certifications such as CCCI: Certified Cyber Crime Investigator, CHFI: Computer Hacking Forensic Investigator, CFCE: Certified Forensic Computer Examiner, CISSP - Certified Information Systems Security Professional, CISA - Certified Information Systems Auditor, CRISC - Certified in Risk and Information Systems Control etc. or their equivalents.

v) MHA has released fund to the States/UTs as part of CCPWC scheme which must be used for organizing capacity building programme for prevention of cybercrime against women & children.

6 **Cyber Crime Prevention:**

Law enforcement agencies are already following the system of foot patrolling in colonies, keeping a watch on vulnerable localities as well as suspects for intelligence gathering and prevention of physical crime. Similar steps are felt necessary for prevention of cyber crime which may include the following:

i) Setup system to monitor deep web which often is a ground for planning, executing nefarious deals by criminals.

ii) Setup/strengthen social media monitoring facility at State Cyber cell with due emphasis on vernacular content.

iii) Alerts/leads generated from monitoring which require further monitoring/action at local level need to be shared with district/local cyber cells through a secure internal network.

iv) Leverage support of private sector and civil society partners in gathering information, and to apply 'intelligence-led' policing to pre-empt and prevent cybercrime.

v) Maintain a list of suspect profiles for monitoring, especially for busting rackets of child pornography, human trafficking and blackmailing etc.

vi) Improve information sharing with other LEAs for expediting prompt action on social media alerts.

7. **Research & Development:**

Technological developments are happening at a very fast pace in Cyber space which pose new challenges. MHA plans to undertake R&D in cyber domain for meeting these emerging challenges. In this regard, all States/UTs are advised to:

i) Identify need for research & development in specific areas of cyber space and regularly update MHA about such requirements.

ii) Suggestions for amendments in legal & policy framework may also be shared with MHA.

8. **Online cybercrime reporting portal:**

In a PIL filed by NGO Prajwala, Supreme Court has issued directions to MHA to create a platform for filing complaints related to cybercrimes online. Accordingly MHA is developing a portal cyberpolice.gov.in, where victims can file complaint related to cybercrime in hassle-free manner. The portal is being integrated with CCTNS and a detailed SOP as per directive of the Supreme Court is being separately issued. Police officers may access this portal using CCTNS login credentials. In addition, States / UTs may facilitate filing of complaints through their citizen portal already developed under CCTNS.

9. Awareness drive:

It has been noticed that due to lack of awareness about the modus operendi of such cyber criminals, a large number of people become victims of various crimes. Properly educating the people through suitable awareness campaign will help in preventing such crimes to a significant extent. In this regards States / UTs may like to undertake the following:

i) Regular awareness campaign advising people not to share their user ID, password, ATM/Credit card PIN, OTPs etc. Help of financial institutions, NGOs, educational institutions, RWAs etc. may be availed to spread such messages.

ii) Awareness focusing on educating the users of cyber space about various channels through which cyber complaints can be filed.

iii) Citizens may be made aware of their duty to inform law enforcement agencies about misuse of cyber space especially if they notice child pornography, obscene material/content on social media or other platforms.

iv) Some illustrative creative designs in print, radio and AV are being developed by MHA which will be made available on MHA website. These can be used by States/UTs or they may develop their own creatives as per need.

10. All the States/UTs Administration are advised to take appropriate steps as indicated above. States / UTs may keep MHA informed about the steps taken by them.

The receipt of this letter may please be acknowledged.

(Kumar Alok)
Joint Secretary (CIS)
January 13, 2018

Copy to;

1. Home Secretaries of all State Governments/UTs.
2. The DGPs of all State Governments/UTs