F. No. 24013/07/Misc/2011-CSR.III
Government of India/ Bharat Sarkar
Ministry of Home Affairs/Grih Mantralaya
****

North Block, New Delhi.
Dated the 4th January, 2012

To,

The Chief Secretaries,
All State Governments/UT Administrations.

Subject: Advisory on Preventing & Combating Cyber Crime against Children.

Sir/Madam,

Introduction

With the spread of computers and internet, cyber-crime has emerged as a major challenge for law enforcement agencies. The younger generations, which use the internet and other online technologies extensively for staying connected for all day to day work and entertainment, including information, e-mails, social Networking, e-banking, e-shopping, web-TV, news, education, home-work research, online gaming, downloading music, videos, movies and other contents etc, are more vulnerable to targeted cyber-crime. This often happens in the form of cyber stalking, cyber bullying, child pornography, harassment, hacking of email or social networking accounts, identity theft, unwanted exposure to sexually explicit material etc. (Brief description of the above terms is attached at Annexure).

2. The following key action points have been worked out in collaboration with various Stake holders for effective prevention and combating of cyber crime against children.

I. The Law Enforcement Agencies i.e. Police, Prosecution and Judiciary etc. and the Public at large may be made aware and trained through special training programmes /seminars and workshops for the effective implementation of Information technology Act, 2000 read with Information Technology (Amendment) Act 2008 and Rules made there under, as these are effective laws to deal with Cyber-Crime, including crime against Children. The training should be with the specific purpose of handling crimes against children.

II. Special Juvenile Police Units constituted under sec. 63 of Juvenile Justice (Care and Protection of Children) Act, 2009 may be sensitized and trained to deal with children in conflict of law with respect to cyber-crimes as well.

III. Parents, teachers & children should be encouraged to play an active role by reporting suspicious behaviour and give information regarding websites hosting exploitative images, videos and efforts to recruit or groom children for sexual abuse. Special precautions will need to be taken to monitor and regulate the spreading awareness of cyber crime among children so that it does not have any negative effect. Use of electronic and print media may also be made appropriately.

IV. It is essential to monitor and regulate social networking sites and services because it has been seen that it hosts most of the obscene materials which induce children to sexually explicit act or other crimes. Parents, teachers and owners of the online computing facilities should be trained to implement "parental control software' in such a manner that spoofing of age, gender and identity is mitigated. In their implementation, multifactoral authentication and other security techniques should be employed.

V. Training to protect and seize digital evidence in a secure manner should be provided to law enforcement agencies and also to examiners of digital evidence.

VI. Maintaining confidentiality of the child victim and providing him/her guidance and support to deal with the after effects of such crimes should be ensured.

VII. Obtaining help and support of NGO's working in the field of online child protection.

VIII. Conducting special sensitization programme and skill development for those manning child help lines such as 1098 or Police Control Room etc. may be considered.

IX. On the State Police websites, social networking websites and web browsers it is suggested to have a children's corner where Internet safety tips in simple language can be explained to them and helpline number or e-mail addresses provided for, in case of any problem.

X. Efforts can be made to develop some mechanism by which online checking of registers, records of each cybercafé can be done from a central location.

XI. Mobile Internet security must be promoted among parents and children.

XII. It is often seen that processing of digital evidence in Computer Forensic Laboratories takes a long time. States must consider as take him their own central as well as regional computer forensic laboratories. Mobile Cyber Forensic Vans would also be useful in seizing electronic evidence from the spot in a proper manner. Assistance of NASSCOM may also be taken to establish cyber labs & training. In addition to NASSCOM help of other agencies like NTRO, CERT-In etc. may also be taken for training.

XIII. In appropriate cases, police officers may carry out undercover cyber patrol operations to identify internet criminals, lure them by posing as minors and arrest them. The exercise should be done in accordance with Section 72 and Section 72 (A) of Information Technology Act, 2000.

XIV. Apart from legal provisions for search under Section 100 and 165 Cr. P. C., Section 80 of IT(Amendment) Act, empowering any police officer not below the rank of a Police Inspector for search, can also be used appropriately.

XV. “Cyber Crime Investigation Manual" published by Data Security Council of India is a useful book and may be referred to.

XVI. Whenever it is noticed that the investigation requires information or help from outside India, CBI Interpol Division may be approached and provision of Mutual Legal Assistance Treaties and Letter of Rogatories (LRs) may be used. Ministry of Home Affairs circular No.25016/14/2007-Legal Cell, dated 31-12-2007, may be referred to for guidelines in this regard. However, it should be kept in mind that LRs are often time consuming and by the time LRs are issued, the digital foot prints (evidence) is already lost. G8 24x7 Desk of CBI, which looks after network and international aspects of cyber crime, may be contacted.

XVII. Wherever any material which is covered under Section 67, Section 67 A and Section 67 (B) of Information Technology Act, 2000 and seen on the Web, which is covered under Section 69 (A) of the IT Act under ‘Public Order’ or ‘preventing incitement to commissioning of cognizable offence’ in such cases, police may consider invoking provisions of IT Procedure and Safeguards for Blocking of Information by Public Rules, 2009. Provisions of Section 67 (C) of IT Act should be used for preservation of evidence by intermediaries.

XVIII. Websites hosting online gaming or children centric contents must issue specific guidelines regarding internet safety. Those transmitting, publishing or

storing obscene material in contravention with the provisions of Section 67, Section 67 (A), Section 69, Section 69 (A) and Section 69 (B) of the IT Act, must be acted against.

XIX. In appropriate cases, police should request Social Networking sites to remove undesirable contents. Most frequently visited and popular sites should be audited for security concerns. Many of these are being used either for compromising of systems or for luring and incitement of children.

3. The aforesaid measures are only indicative and the State Governments/UT Administrations may consider any additional measures for the preventing & combating cyber crime against children as necessary. This Ministry may also be kept apprised of any special measures/mechanisms introduced in their respective jurisdictions so that the same could be circulated to the other State Governments and UT Administrations for consideration/ adoption.

4. The receipt of this letter may kindly be acknowledged.

Yours faithfully,

(B. Bhamathi)
Additional Secretary to the Govt. of India,
Tele No. 23092514.

Copy for information and necessary action to:-

1. The Principal Secretary/ Secretary Home – All State Governments/UT Administrations.

2. The Director General of Police – All State Governments/UT Administrations.

Annexure

(a). **Cyber Stalking :** When a victim is repeatedly and persistently followed and pursued online by e-mail or other electronic communication. In such crimes Sections 66A, 66C and 66E of Information Technology Act along with Section 506, 509 IPC can be invoked depending upon the nature and facts of the case.

(b). **Cyber Bullying:** Acts of harassment, embarrassment, taunting, insulting or threatening behaviour towards a victim by using internet, e-mail or other electronic communication device. In such crimes Sections 66A, 66C and 66E along with Section 506, 509 IPC can be invoked depending upon the nature and facts of the case.

(c). **Child Pornography:** This has been defined in Section 67B of IT Act. Section 67 and 67A and Section 292, 293 IPC can also be invoked as per the facts of the case.

(d). **Hacking of E-mails or social networking accounts:** Unauthorized use or access to the e-mail or social networking accounts such as Facebook, Orkut, Gmail, Hotmail etc. Section 43 and 66C of IT Act can be invoked.

(e). **Identity Theft:** Has been defined in Section 66C of IT Act which can be invoked.

(f). **Unwanted exposure to sexually explicit material etc.:** When a criminal sends pictures, videos, sound clips, cartoons or animations depicting sexual contents by e-mail or any other electronic means. This would include audio or video chat using web camera etc.

1. Section 66 A of IT Act needs to be invoked whenever any offensive, annoying or threatening email, SMS or MMS etc. are received by children who are victims of cyber bullying or stalking.

2. Section 67 B of IT Act must be used when the electronically published or transmitted material contain child pornographic material. The Section also prohibits grooming of children for sexual abuse etc.

3. Section 66 A of IT Act may be invoked when ever email or social networking accounts of a child are hacked by misusing passwords or his/her photographs, name and other unique identification feature are misused.

4. Section 66 E of IT Act can be used for violation of bodily privacy of a person.

5. Section 67 and 67 A of IT Act can be used when ever pornographic material has been received by children by Email or SMS/MMS or other electronic means.

----x----