

*Pls circulate to all including field formations. 2/16/12*

GOVERNMENT OF PAKISTAN  
CABINET DIVISION  
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD  
(NTISB)  
\*\*\*\*\*

No. 1-4/93(NTISB)

Islamabad 10 July 2012

Subject:- Use of Cellular Mobile Phones and its Security Hazards

*11 JUL 2012*  
*M(A)*  
*SA/PS*  
*2/16/12*  
*33 Coords*  
*2/16/12*  
*MM*

Rapid pace and advent of new technologies in telecom sector has transformed the world as a whole and this revolution has eased the human life to a large extent. Cellular phone technology has widened the scope of communication in voice and data exchange which added new dimension to the emerging technology. Over a decade or so, this rapidly increasing technology has brought multiple voice/data features namely voice/data chatting, faster broad band application, easy touch and play system, e-businesses/banking management and many other social and global internet applications. With high versatility, usage and diverse application, this facility is being used by not only common citizens but also government officials/statesmen. At present this technology is providing multiple services to the people around the globe and its economy has grown manifold than any other technology in the world. Positive use of such emerging technologies has also facilitated the human society at large, however being a double edged weapon with sophisticated communication tools, it also has some inherent security weaknesses/draw backs which has negative impacts on our day to day activities. Some of the vital areas of concern regarding misuses of cellular phones have been briefly explained in succeeding paras:-

- a. Most of the mobile phones have inbuilt camera facility with higher resolution imaging system for both photo and video recording which can not only be mutilated for any possible blackmailing/ defaming but mobile phone camera may also be used for recording of sensitive document/ data and hence may result in serious security lapses and consequences.
- b. Internet and fast ethernet broad services are the most common applications which are easily accessible in cheaper commercial tariffs

97716-R  
FBR CDX Dy. No. \_\_\_\_\_  
Received in JCH Unit.  
on 11 JUL 2012

*6/32 1.2.2012*

to facilitate the masses but can also be materialised for any purpose including hacking, blasphemous, vulgarity, e-mail viruses and misuse of data transfer/ sharing.

- c. Since the cell phone sets have inbuilt microphone facility with higher sensitivity and fidelity, these cell phones can be remotely operated, therefore any high level meeting/conversation can be easily tapped, which subsequently can be quoted in any court of law and hence may cause serious risks to the user organization.
- d. Where on one hand, this rapidly advancing multi-billion dollar technology provides speedy and clear transfer of public data/voice services, it is also easily susceptible to eavesdropping/ interception by hostile agencies which may pose serious threat.
- e. In case of few cell phones the data/ text messages by the users are routed through the servers placed abroad where a copy of text/ data is stored thus may pose risk to the privacy of user as well as his organization.
- f. The stolen/ lost cell phone can be used by the terrorist/ miscreant for malafied purpose.
- g. The cell phone data including contact numbers can be easily hacked/ modified and misused by the interested parties.

3. Keeping in view the increasing misuse and related security hazards, following is recommended:-

- a. Cell phones must not be allowed to be carried in any official meetings.
- b. No official data may be stored in the cell phones.
- c. Cell phones must be prohibited at sensitive places/ offices.
- d. Cell phones may not be used for official/ sensitive conversation and exchange of data.

- e. Since the cell phones even when switched off can be remotely switched "ON" therefore strict cell phones carrying/ usage policy may be enforced by all ministries/ government departments/ organizations and agencies.
- f. All ministries/ government departments/ organizations and agencies may formulate their SOPs on fair use of cell phones.
4. Apropos, it is felt necessary that all Ministries/Divisions/Govt departments/offices may sensitize their employees to be well aware/ educated on advanced mobile/ cell phone technology and be vigilant of their open usage/related hazards while sharing sensitive voice/data communication in the public.



Lt Col  
(Malik Nadeem Akhtar)  
Deputy Secretary (NTISB)

All PS to Secretaries of Federal Ministries/ Divisions