3. Etisalt DB Telecom Private Limited

4. Idea Cellular Limited

5. Reliance Communications Limited

6. S Tel Private Limited

7. Tata Teleservices Limited

8. Videocon Telecommunications Limited

9. Vodafone Essar Cellular Limited

Statement-II

Details of notices for inviting application for auction of spectrum

S.No.	Activities	Dates
1.	Last date for submission of applications	March 19, 2010
2.	Publication of ownership details of applicants	March 23, 2010
3.	Bidder ownership compliance certificate	March 26, 2010
4.	Pre-qualification of bidders	March 30, 2010
5.	Mock auction	April 5-6, 2010
6.	Start of 3G auction	April 09, 2010
7.	Closing of 3G auction	May 19, 2010

Statement-III

Name of the Successful Bidders in 3G Auction

1. Aircel Limited

2. Bharti Airtel Limited

3. Etisalt DB Telecom Private Limited

4. Reliance Communications Limited

5. S Tel Private Limited

6. Tata Teleservices Limited

7. Vodafone Essar Cellular Limited

Cyber crime in India

421. SHRI R.C. SINGH: Will the Minister of COMMUNICATION AND INFORMATION TECHNOLOGY be please to state:

(a) whether it is a fact that as per the Report of the Symantec's Cyber Crime Countries, India stands at 5th Place in 2009 from 11th in 2008;

(b) whether it is also a fact that the cyber attackers are targeting social networking sites to steal the data; and

(c) if so, in what manner Government is planning to contain the cyber attacks?

THE MINISTER OF STATE IN THE MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY (SHRI SACHTN PILOT): Yes Sir. Symantec is a US Company engaged primarily in Antivirus and other security products. They release Internet Security threat reports regularly. In the latest report (for the year 2009) dated April 2010, malicious activity by country has been mentioned wherein India is ranked at No. 5 as compared to No. 11 in the year 2008.

The findings of such reports by security vendors are generally based on data generated by their products and vary drastically in their findings.

Such security reports are also released by other Antivirus and software companies. The details of research data is not shared by them and hence can not be verified.

(b) Social networking sites are gaining popularity. Like any other service or application, social networking sites are also misused for malicious purposes. The attackers create fake or untraceable profiles for joining groups of benign users and harvest information and use it for malicious purposes. Social networking sites are also used by certain malicious code/worms for propagation and information stealing.

(c) The Government has taken several measures to detect and prevent cyber attacks.

1. The Information Technology Act, 2000 as amended by the Information Technology (Amendment) Act, 2008 has been enforced on 27.10.2009. The Act provides legal framework to address the issues connected with hacking and security breaches of information technology infrastructure.

2. The Indian Computer Emergency Response Team (CERT-In) scans the Indian Cyber Space to detect traces of any untoward cyber incident. CERT-In performs both proactive and reactive roles in computer security incidents prevention, identification of solution to security problems.

   CERT-In regularly publishes Security Guidelines and advisories for safeguarding computer systems from hacking and these are widely circulated. All Government Departments/Ministries, their subordinate offices and public sector undertakings have been advised to implement these guidelines to secure their computer systems and information technology infrastructure.

CERT-In also conducts security workshops and training programs on regular basis to enhance user awareness.

3. CERT-In has also published a Security Guideline for general users on "Securing Home Computers". The Guideline makes a user aware about the latest security threats and provides information to install anti-virus software and other security protection tools onto his/her home computer system for safeguarding against cyber attacks. A portal "secureyourpc.in" is created to educate consumers on cyber security issues.

4. The Government has formulated Crisis Management Plan for countering cyber attacks and cyber terrorism. For implementation by all Ministries/Departments of Central Government, State Governments and their organizations and critical sectors.

5. The organizations operating critical information infrastructure are regularly advised to implement information security management practices based on International Standard ISO 27001.

6. Ministries and Departments have been advised to carry out their IT systems audit regularly to ensure robustness of their systems. CERT-IN has already empanelled a number of penetration testing professionals through a stringent mechanism of selection to carryout audits.

Auction of 3G spectrum

422. SHRI KALRAJ MISHRA: Will the Minister of COMMUNICATIONS AND INFORMATION TECHNOLOGY be pleased to state:

(a) the amount of money that had been collected by his Ministry through the auction of 3 G spectrum;

(b) in what manner his Ministry proposes to spend this money for the development of communication network particularly in rural areas of the country;

(c) the estimated loss in auction of 2G spectrum in view of the collection recorded in 3G auction;

(d) whether irregularities have been detected in the auction of 2G spectrum; and

(e) if so, the action taken so far in this regard?

THE MINISTER OF STATE IN THE MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY (SHRI SACHIN PILOT): (a) Total amount of money earned by the auction process is Rs. 67,718.95 crores from 3G spectrum.