- It will provide an access to the capital market for raising fresh equity capital, if required.
- It will facilitate BSNL to get Navratna status.

The timing of the issue depends on the conditions of the capital market.

(c) and (d) Sir, the main parameter for adjudging the financial position of a Company is the networth, which has not declined in the case of BSNL. However, there is considerable decline in Profit After Tax (PAT), since the year 2005. The details of the net worth & PAT for the last five financial years are as follows:-

Financial Year	Net Worth	Profit After Tax
2004-05	72779	10183
2005-06	80757	8940
2006-07	86948	7806
2007-08	88128	3009
2008-09	88634	575

(e) BSNL has undertaken organization restructuring with the help of a management consultancy firm the "Boston Consulting Group" to provide end-to-end focus on core businesses *viz.* mobile, fixed access, enterprise and new businesses. Further, a Committee constituted by the Government under the Chairmanship of Shri Sam Pitroda has submitted its report in the matter.

Discussion of Afghanistan in Istanbul

*57. SHRI TIRUCHI SIVA: Will the Minister of EXTERNAL AFFAIRS be pleased to state:

(a) whether Government is aware of the outcome of the recent meeting of certain countries on Afghanistan which took place in Istanbul;

(b) the countries that attended the meeting;

(c) the reasons for excluding India from such a meeting;

(d) whether Government has taken up the issue with the host country; and

(e) if so, the response thereto?

THE MINISTER OF EXTERNAL AFFAIRS (SHRI S.M. KRISHNA): (a) and (b) Turkey hosted the fourth trilateral Summit of the Presidents of Afghanistan, Turkey and Pakistan on January 25, 2010. A Regional Conference was held in Istanbul on January 26, 2010 with participation from Iran, Tajikistan, Uzbekistan, China, Turkmenistan, Pakistan, Afghanistan and Turkey. A number of other countries/organizations were invited to be observers and included the US, UK, Germany, France, Russia, Japan, Kyrgyzstan, UAE, Saudi Arabia, OIC, Italy, UN, NATO, EU and ECO.

i) 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.

ii) The organizations operating critical information infrastructure have been advised to implement information security management practices based on International Standard ISO 27001.

iii) Ministries and Departments have been advised to carry out their IT systems audit regularly to ensure robustness of their systems. Indian Computer Emergency Response Team (CERT-In) has already empanelled a number of penetration testing professionals through a stringent mechanism of selection to carry put audits.

iv) National Informatics Centre (NIC) is continuously strengthening the security of the network operated by them and its services by enforcing security policies, conducting regular security audits and deploying various technologies at different levels of the network to defend against the newer techniques being adopted by the hackers from time to time.

v) 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.

Section 70 of the Act provides for declaration of any computer resource, which directly or indirectly constitutes Critical Information Infrastructure, to be a protected system.

Further, Section 70B has empowered Indian Computer Emergency Response Team to serve as national nodal agency in the area of cyber security.

vi) The Indian Computer Emergency Response Team (CERT-In) scans the Indian Cyber Space to detect traces of any untoward incident that poses a threat to the cyber space. CERT-In performs both proactive and reactive roles in computer security incidents prevention, identification of solution to security problems, analyzing product vulnerabilities, malicious codes, web defacements, open proxy servers and in carrying out relevant research and development.

Sectoral CERTs have been functioning in the areas of defence and Finance for catering to these critical domains. They are equipped to handle and respond to domain specific threats emerging from the cyber systems.

CERT-In has published several Security Guidelines for safeguarding computer systems from hacking and these have been 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 issues security alerts, advisories to prevent occurrence of cyber incidents and also conducts security workshops and training programs on regular basis to enhance user awareness.