(c) whether it is also a fact that this led to the decline of BSNL market share in mobile segment;

(d) whether Government undertook any inquiry to find out the reasons for halving the tender;

(e) if so, the findings thereof; and

(f) if not, the reasons therefor?

THE MINISTER OF STATE IN THE MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY (SHRI GURUDAS KAMAT): (a) and (b) Sir, a period of about one and half year had elapsed from the date of the floating of the tender and finalization of the same and during this period certain significant changes in the telecom service sector had taken place, including technological changes, launching of initiative of sharing of infrastructure by the operators and applicability of USO fund subsidy to mobile services. Accordingly, it was decided by BSNL Board to procure 22.75 million GSM capacity instead of 45.5 million.

(c) No, Sir.

(d) BSNL was asked to comment on the Central Vigilance Commission's letter wherein question has been raised on reducing the procurement quantity under Phase V tender.

(e) and (f) BSNL has explained that about one and half year had elapsed from the date of the floating of the tender and finalization of the same and during this period, certain significant changes in the telecom service sector had taken place, including technological changes, launching of initiative of sharing of infrastructure by the operators and applicability of USO fund subsidy to mobile services.

Contract to Chinese company

4469. SHRI SATYAVRAT CHATURVEDI: Will the Minister of COMMUNICATIONS AND INFORMATION TECHNOLOGY be pleased to state:

(a) whether there are any directions to avoid contracts of sensitive works to Chinese companies;

(b) whether it is a fact that BSNL has given a contract to a Chinese company to lay mobile network of two and half crore lines;

(c) whether it is also a fact that IB and RAW had objected the award of contract to Chinese company;

(d) the officials who played vital role in awarding the said contract; and

(e) whether the role of concerned officers has been investigated by Government, if so, the details thereof?

THE MINISTER OF STATE IN THE MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY (SHRI GURUDAS KAMAT): (a) Sir, in the interest of national security, the

Government has directed Bharat Sanchar Nigam Limited in May, 2009 that resources should not be procured from the Chinese vendors for deployment in the sensitive regions of Assam, Tripura, Sikkim, Nagaland, Arunachal Pradesh, Mizoram, Meghalaya, West Bengal, Gujarat, Rajasthan, Punjab, Jammu and Kashmir, Himachal Pradesh, Uttarakhand and Maharashtra.

Also, amendments have been issued in December, 2009 in the Licence Agreements of all Telecom Service Providers for security related concerns stipulated that the LICENSEE(s) shall apply to the Licensor for security clearance, also with the details of the equipments(s) as well as details of equipments(s) suppliers and manufacturers including Original Equipments Manufacturers (OEM), before placement of the final purchase order for procurement/ upgradation of equipment/software for provision of telecommunications services under the licence and that it shall also include any such activity by the franchisee, agents or person of the licensees. In case no response is received from the Licensor within thirty working days, it shall be presumed that there is no objection to the procurement.

(b) No, Sir.

(c) to (e) Do not arise in view of (b) above.

Cyber espionage in Indian computer system

4470. SHRI P. RAJEEVE: Will the Minister of COMMUNICATIONS AND INFORMATION TECHNOLOGY be pleased to state:

(a) whether Government has taken any steps to prevent cyber espionage network hacking into computer systems of Indian Government;

(b) if so, the details of the preventive measures taken; and

(c) whether preventive steps had been extended to several Indian Embassies abroad?

THE MINISTER OF STATE IN THE MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY (SHRI SACHIN PILOT): (a) and (b) The Government has taken several measures to detect and prevent cyber attacks/espionage. The details are:—

1. As per existing computer security guidelines issued by Government, no sensitive information is to be stored on the systems that are connected to Internet.

2. 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.

3. The organizations operating critical information infrastructure have been advised to