DEFEN THE SECHETARY

FOURTEENTH CONGRESS OF THE REPUBLIC) OF THE PHILIPPINES

First Regular Session

7 557 -7 11 "

SENATE P.S. Reso. No. MECENEE ST.

Introduced by Senator Lacson

RESOLUTION

DIRECTING THE COMMITTEE ON NATIONAL DEFENSE AND SECURITY TO CONDUCT AN INQUIRY IN AID OF LEGISLATION INTO THE NATIONAL SECURITY IMPLICATIONS OF AWARDING THE NATIONAL BROADBAND NETWORK CONTRACT TO THE CHINESE FIRM ZHONG XING TELECOMMUNICATIONS EQUIPMENT COMPANY LIMITED (ZTE CORPORATION), WITH THE END IN VIEW OF PROVIDING REMEDIAL LEGISLATION THAT WILL FURTHER PROTECT OUR NATIONAL SOVEREIGNTY AND TERRITORIAL INTEGRITY.

Whereas, in September 2006, Zhong Xing Telecommunication Equipment Company Limited, otherwise known as ZTE Corporation submitted to the Commission on Information and Communication Technology (CICT) an unsolicited proposal for a National Broadband Network (NBN);

Whereas, ZTE Corporation, originally established as Zhongxing Semiconductor Co. Ltd. in February 1985, is the largest publicly-listed telecoms manufacturer in China with shares publicly traded in both the Hong Kong and Shenzhen Stock Exchange. As of December 31, 2005, the Chinese Government (through Zhongxing) owned 37.41% of ZTE;

Whereas, the group is engaged in the design, development, production, distribution, and installation of advanced telecommunications systems and equipment, including wireless communications systems, wireline switches, and access equipment, optical and data communications equipment, handsets, and telecommunications software systems and services;

Whereas, on April 21, 2007, a \$329,500,000.00 million contract for the National Broadband Network (NBN) financed by way of a loan from the Export-Import Bank of China was signed between Department of Transportation and Communications (DOTC) Secretary Leandro Mendoza and ZTE's Vice President, Yu Yong;

Whereas, the NBN proposed project consist of two main components, to wit: (a) the NBN Infrastructure which involves the design, site preparation, installation, and commissioning for all the network technical subsystems of the NBN architecture. Training on the management, testing, operation and maintenance of the system will also be provided and (b) the NBN Application System/Services which will primarily provide Voice over Internet Protocol (VoIP) service to all government offices and video conferencing systems to provide real time inter-office conferencing and other value added services like CERS for disaster alerts, and E-Government System for integrated government internet portal and technology platform;

Whereas, there has been a huge public outcry to repudiate this project for alleged violations of the following: (1) the rule on public bidding as required under Republic Act No. 9184; (2) it contradicts—the long standing policy of government to give preference

to private enterprise in the operation and maintenance of infrastructure and development projects; (3) existing private consumers of this medium will be adversely affected because of the sure increase in the rates for said services to cover the huge income private providers will lose because of the NBN and lastly, (4) the existence of other offers where the government does not have to spend a single centavo, or add to our already huge public debt;

Whereas, a very important consideration had been overlooked in the discussions of this proposed project, i.e. the national security implications of an NBN that will be built by a foreign government considering that national security matters, state secrets and other confidential information will logically be coursed through this medium of communication once the same is already operational;

Whereas, this apprehension is well-founded in view of our recent experience involving our own military intelligence service conducting wiretapping activities using very crude means as well as the reported hacking of the defense network of the Pentagon by the Chinese People's Liberation Army which led to the shutdown of the computer system serving the office of US Defense Secretary Robert Gates. Likewise reported was the alleged hacking of the German computer system to include the computer system of Chancellor Angela Merkel, the German foreign ministry office and other government agencies in Berlin by the same group;

Whereas, we should also take note of the fact that at present, both the governments of the Philippines and China are having contrary and conflicting claims over a group of islands otherwise known as the Spratly Islands;

Whereas, with this system being built by a firm owned by a foreign government reported to have engaged in illegal hacking of government agencies even of First World countries, there is reason for grave concern about unrestricted access to military and other confidential information passing through the NBN that might compromise our national security and interests;

Whereas, it is imperative therefore that this type of contract, if there exists a need for one, should be limited to Filipino companies that can easily be held liable for violating our laws;

Whereas, this policy is in consonance with Section 7, Article II of the 1987 Constitution which mandates the state to pursue an independent foreign policy and that in its relations with other states the paramount consideration shall be national sovereignty, territorial integrity, national interest and the right to self determination and also with Section 10, Article XII which mandates that "in the grant of rights, privileges and concessions covering the national economy and patrimony, the state shall give preference to qualified Filipinos;" NOW, THEREFORE, BE IT

RESOLVED AS IT IS HEREBY RESOLVED, to direct the Committee on National Defense to conduct an investigation in aid of legislation, on the contract entered into by the Philippine government with ZTE Corporation, with the end in view of primarily examining the security implications of the said deal in light of the highly sensitive nature of the information that will flow through the NBN and at the same time provide remedial legislations that will address the above-mentioned situations and potential threats.

Adopted,