Congress of the United States
House of Representatives
Washington, D.C. 20515

Anna G. Eshoo
Fourteenth District
California

1743

November 2, 2010

The Honorable Julius Genachowski, Chairman
Federal Communications Commission
445 12th Street, S.W.
Room 8B201
Washington, D.C. 20554

Dear Chairman Genachowski,

As a senior member of the House Permanent Select Committee on Intelligence, I have had grave concerns about the implications of foreign-controlled telecommunications infrastructure companies providing equipment to the U.S. market for quite some time. In particular, I'm very concerned that Huawei and ZTE, Chinese telecommunications infrastructure manufacturers are looking to increase their presence in the U.S.

These companies have long-standing relationships with the Chinese People's Liberation Army, and are not subject to the same kinds of independence and corporate transparency that other countries require of their telecommunications companies.

Last May, I wrote to the Director of National Intelligence and asked him to assess the national security implications of Chinese-origin telecommunications equipment on our law enforcement and intelligence efforts, as well as on our switched-telecommunications infrastructure. While I cannot discuss the results of that assessment in an unclassified letter, suffice to say the answers were troubling, and the National Counter Intelligence Executive has made communications infrastructure security a top priority.

Huawei and ZTE have recently taken aggressive steps to increase penetration into the U.S. telecommunications market. This summer, Huawei was in discussions with Sprint to provide mobile telecommunications equipment. And in August of 2009, Huawei signed a deal with Clearwire to provide equipment to their wireless network. Unlike mergers and acquisitions by foreign firms, agreements to directly supply equipment to the U.S. telecommunications infrastructure are not subject to CFIUS requirements.

However, the net result is the same, where sensitive U.S. communications will travel over the networks and switches provided by a foreign-controlled entity.

Clearly, the current CFIUS regime does not provide scrutiny of procurements from foreign companies to assess the risk to the U.S. telecommunications infrastructure. I would like to understand what your role is to protect the U.S. networks in order to assess what additional legislation may be needed.

- Do you have authority to protect the U.S. telecommunications infrastructure from inappropriate foreign control or influence?

- What authorities do you have to review procurements of foreign equipment by U.S. companies operating our telecommunications networks? What additional authorities would you need to ensure that the U.S. telecommunications infrastructure is secure from foreign influence?

- To what extent are you working with our nation's intelligence community to assess the threat to our telecommunications infrastructure? What is, or should be, the interagency structure to best review procurements from foreign entities?

- What kinds of transparency requirements, including divestment from state ownership, should be placed on companies seeking to sell telecommunications infrastructure equipment to U.S. network providers? Should this be a U.S. or an international standard?

Our nation's telecommunications infrastructure must be protected for our national security, and I look forward to your prompt reply.

Sincerely,

Anna G. Eshoo
Member of Congress

cc: The Honorable James Clapper, Director of National Intelligence
The Honorable Leon Panetta, Director, Central Intelligence Agency
General Keith Alexander, Director, National Security Agency