Congress of the United States

Washington, DC 20510

October 19, 2010 **1670**

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

Dear Chairman Genachowski:

We write to request information concerning the FCC's plans for ensuring the security of our nation's telecommunications networks. As you are aware, two Chinese companies, Huawei Technologies Co., Ltd. and ZTE Corporation, are aggressively seeking to supply sensitive equipment for U.S. telecommunications infrastructure and/or serve as operator and administrator of U.S. networks, and increase their role in the U.S. telecommunications sector through acquisition and merger. We understand they are in active discussions with two U.S. companies – Sprint and Cricket – and other prospective deals may be on the horizon. The sensitivity of information transmitted in communications systems, as well as the potential for foreign espionage, requires that the U.S. government take decisive action to ensure the security of our telecommunications networks.

Huawei and ZTE are among the largest manufacturers of sensitive telecommunications equipment in the world. In fact, the *New York Times* reported in November that Huawei is now the world's second largest telecommunications equipment manufacturer. A 2009 report by the Department of Defense (DOD) and a 2005 report from the RAND Corporation state that Huawei has significant ties to the Chinese military, the People's Liberation Army (PLA). In addition, both companies have, according to published reports, received tens of billions of dollars in export financing and "low- to no-interest 'loans' that needn't be repaid" from the Chinese government.[1]

We are very concerned that these companies are being financed by the Chinese government and are potentially subject to significant influence by the Chinese military, which may create an opportunity for manipulation of switches, routers, or software embedded in American telecommunications network so that communications can be disrupted, intercepted, tampered with, or purposely misrouted. This would pose a real threat to our national security. We understand that other governments, including those of the United Kingdom, Australia, Canada, and India may already have raised such concerns.

---

[1] CNN Money.com, "China's new frontier. Chinese telecom-gear makers Huawei and ZTE have already conquered Africa and Asia. Next stop: Latin America." June 25, 2009.

In addition, changes in the telecommunications market are causing domestic carriers to outsource their network operations to telecommunications equipment suppliers. So it is possible that U.S. telecommunications will be managed in whole or in part from China or by Chinese nationals if the market is unconstrained. This trend has already emerged in the telecommunications networks of many of our closest allies, including those with whom we conduct sensitive intelligence activities.

While Huawei and ZTE have in the past focused on other parts of the world, they have recently taken aggressive steps to increase penetration into the U.S. telecommunications market. Huawei, for example, has made several bids to supply telecommunications equipment at low prices with attractive financing, and it has been making more sales of late. Deals to directly supply equipment to the U.S. telecommunications infrastructure are, of course, not subject to CFIUS requirements, which only apply when a foreign firm is seeking to purchase or obtain a controlling interest in a U.S. company that is deemed to have a national security consequence. But when telecommunications carriers purchase equipment from Huawei, the result is that U.S. communications will travel over switches, routers, and other equipment that was manufactured and designed in China and may be remotely accessed and programmed from that country, and the CFIUS process cannot protect against it.

Given the role of the FCC, and its requirement to take actions to protect the public interest, we would like to know what the FCC is doing to protect the U.S. telecommunications system and would appreciate your prompt and detailed response to the following questions:

1) Does the FCC have the legal authority to review (in consultation and coordination with other agencies) foreign technologies, including equipment and software, to determine the risk posed to U.S. telecommunication networks? Is it doing so? How?
2) Does the FCC work with the Department of Homeland Security or the Intelligence Community to better understand potential risks posed to U.S. telecommunications networks? What is the mechanism for this consultation?
3) Does the FCC believe there are risks to U.S. telecommunications carriers buying foreign technology that may subject U.S. telecommunications networks to increased risk of espionage or interference with operations? What are those risks? Has the FCC so advised U.S. telecommunications carriers of these risks? Specifically, has the FCC had any discussions with Sprint or Cricket about the transactions they are considering with Huawei, according to reports? And has the FCC considered whether there should be limitations on foreign equipment employed in the proposed build out of the 700 MHz "D" Block of spectrum that may be used to provide a broadband network for public safety?
4) Has the FCC monitored the sale of foreign telecommunications equipment, software or services to U.S. carriers? How much of this equipment has been manufactured, produced or provided by companies like Huawei and ZTE that are closely linked to a foreign government and/or foreign military? Which U.S. telecommunications companies have purchased it? (Please include a detailed analysis of the geographic regions covered by those networks.)
5) Does the FCC have information, or has it seen reports, that ZTE and Huawei are subsidized – e.g., including low- or no-interest loans, loan forgiveness, or restrictions

on access to People's Republic of China (PRC) or PLA procurement markets – by the PRC? Has it shared or sought this information through the U.S. Trade Representative or Department of Commerce and asked either office to investigate unfair trade practices for potential WTO violations? Does the FCC believe such subsidies create an unfair advantage over U.S. firms for Huawei and ZTE?

6) Does the FCC believe there are risks of outsourcing to foreign companies the responsibility for operating and administering U.S. telecommunications carrier networks? Please explain what the FCC has determined are those risks. Has the FCC so advised U.S. telecommunications carriers about these risks? What steps has the FCC taken to mitigate those risks?
7) Please describe in detail whether the effective implementation of the Communications Assistance for Law Enforcement Act (CALEA) is impacted by outsourcing to foreign companies the responsibility for operating and administering U.S. telecommunications carrier networks. Is effective implementation of CALEA impacted by the provision of telecommunications equipment, software, or services used by U.S. telecommunications companies by foreign companies tied to foreign militaries or foreign governments? What policies has the FCC adopted to deal with these impacts?

We appreciate your responses and your service to ensure the security of U.S. telecommunications networks.

Sincerely,

JON KYL
United States Senator

JOSEPH I. LIEBERMAN
United States Senator

SUSAN M. COLLINS
United States Senator

SUE MYRICK
United States Representative

CC: The Honorable Janet Napolitano, Secretary, Department of Homeland Security
The Honorable Ron Kirk, United States Trade Representative
The Honorable Robert Mueller, Director, Federal Bureau of Investigation