Fears of spying hinder China Mobile license

May 11 2012, By Ken Dilanian

Concerned about possible cyber-spying, U.S. national security officials are debating whether to take the unprecedented step of recommending that a Chinese government-owned mobile phone giant be denied a license to offer international service to American customers.

China Mobile, the world's largest mobile provider, applied in October for a license from the Federal Communications Commission to provide service between China and the United States and to build facilities on American soil.

Officials from the FBI, the Department of Homeland Security and the Justice Department's national security division are concerned that the move would give the company access to physical infrastructure and Internet traffic that might allow China to spy more easily on the U.S. government and steal intellectual property from American companies, according to people familiar with the process who declined to be identified because the deliberations are secret.

Those officials, known collectively as "Team Telecom," review FCC applications by foreign-owned companies. They could advise the FCC not to issue the license, but may instead demand a signed agreement designed to satisfy security concerns, the people said.

The review is being led by the Justice Department, which declined to comment, as did the FBI and DHS.

A move to block the license could provoke a lawsuit by China Mobile,

officials said. But lately, the U.S. government's focus on cyber espionage has sharpened considerably.

China Mobile, which has nearly 670 million subscribers, is not applying to provide domestic U.S. telephone or Internet service. But traffic from U.S. carriers, such as Verizon Communications Inc. or AT&T Inc., could be routed to the China-owned network should a license be granted.

"Suddenly, you've got a perfect ability to exfiltrate information out of the country," said Scott Aken, a former FBI cyber security investigator.

A U.S. representative for China Mobile, who declined to be quoted by name, said the company is cooperating with Team Telecom's inquiries and expects to satisfy any concerns through a national security agreement. The firm declined to address allegations about Chinese spying.

Team Telecom's review of China Mobile's application is complicated by the fact that two other Chinese government-owned firms, China Telecom and China Unicom, were granted similar licenses in 2002 and 2003, respectively, well before Chinese cyber espionage was viewed as a pressing concern. Both carry phone and Internet traffic between the U.S. and China.

In neither case did Team Telecom require a national security agreement that specifies, for example, how the company must protect U.S. classified information that could traverse its network.

In recent years, Team Telecom has required foreign-owned firms to sign extremely detailed agreements.

One signed in September by Level 3 Communications, a Broomfield, Colo., carrier, requires the company to provide the manufacturer name

and model number of all equipment relating to the undersea cables used to carry traffic to and from the United States. According to the FCC, 43.5 percent of the company is indirectly owned by foreign interests.

U.S. officials in recent months have warned repeatedly that cyber espionage, in some cases authorized at the highest levels of the Chinese government, has become a grave threat to U.S. economic and national security.

Tens of billions of dollars in U.S. intellectual property has been stolen, much of it through hacking originating in China, U.S. intelligence officials have said. In addition, China has obtained national defense information, the officials have said.

On April 8, 2010, China Telecom, China's largest fixed-line telephone company, rerouted 15 percent of the world's Internet's traffic through Chinese servers for 18 minutes, according to the U.S.-China Economic and Security Review Commission.

China Telecom denied hijacking Internet traffic, but it did not explain how erroneous instructions were issued in a global Internet routing system based largely on trust.

In February 2011, the U.S. government blocked a deal by another Chinese telecom company, Huawei Technologies, to purchase 3Leaf Systems, an insolvent technology firm based in Santa Clara, Calif. Huawei is privately owned, but American officials alleged that it has ties to the Chinese military.

Last month, Australia barred Huawei from bidding for work on its national broadband network because of security concerns. Also last month, Symantec Corp. unwound its joint venture with Huawei, reportedly over concerns that the U.S. government would stop sharing

information with Symantec.

The House intelligence committee is investigating the role of Chinese telecommunications companies in espionage, with a focus on Huawei and ZTE Corp., which makes switches, routers and other products.

Sean McGurk, a former senior DHS cyber security official, said China Mobile's entrance into the U.S. market "would pose a concern to most people. We're not really sure, not only where the information is flowing, but what potentially is being left behind."