Bloomberg Law

Professional Perspective

Risk-Based Security Evaluation of Foreign Wireless Providers and Suppliers

Angela E. Giancarlo, Mayer Brown

Risk-Based Security Evaluation of Foreign Wireless Providers and Suppliers

*Contributed by Angela E. Giancarlo, Partner, Mayer Brown**

U.S. and Chinese companies are aggressively competing to achieve global leadership in Fifth Generation ("5G") technology and deployments. The winner will receive trillions of dollars in economic benefits, which includes the personal and other sensitive data collected by these connected devices. The key question for U.S. policymakers (and ultimately for broadband service providers and their suppliers) is how to ensure that foreign entities, including those from China, cannot sabotage the security of these vital 5G networks, steal personal information, engage in espionage, and disrupt communications services.

Introduction and background

5G wireless networks are expected to increase data speeds by 100 times, support billions of Internet of Things devices, and provide near-instant universal wireless coverage and availability. More specifically, 5G networks will be the backbone of tomorrow's economy. These connections will empower a vast array of new critical services—everything from autonomous vehicles and transportation systems, electricity grids, remote surgery, and battlefield communications will be built on 5G foundations.

Recent actions by the Administration and the Federal Communications Commission ("FCC") exemplify the federal government's recognition that a risk-based security approach must include a heightened evaluation of service providers and suppliers of hardware and software. This new approach includes scrutinizing the extent to which foreign entities are controlled by their governments and whether the governments would have unfettered authority over their business decisions and activities.

Executive Order 13873

On May 15, 2019, President Trump issued Executive Order 13873, Securing the Information and Communications Technology and Services Supply Chain ("EO"), which authorizes the U.S. Secretary of Commerce, in consultation with the Secretaries of Treasury, State, Defense, Justice, Homeland Security, and the Chairman of the FCC, the U.S. Trade Representative, the Director of National Intelligence, and the Administrator of General Services, to take collective action to ensure the integrity of U.S. communication networks.

Based on a finding that "foreign adversaries are increasingly creating and exploiting vulnerabilities in information and communications technology and services, which store and communicate vast amounts of sensitive information, facilitate the digital economy and support critical infrastructure and vital emergency services," the EO directs additional steps "to deal with this threat."

The Executive Order prohibits certain transactions involving information and communications technology or services where:

> (i) the transaction involves information and communications technology or services designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary; and
>
> (ii) the transaction:
>
> > (A) poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of information and communications technology or services in the United States;

(B) poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the digital economy of the United States; or

(C) otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons.

In a statement, Commerce Secretary Wilbur Ross said the action would "prevent American technology from being used by foreign-owned entities to potentially undermine U.S. national security or foreign policy interests."

FCC denies China Mobile application for authority to provide service in the U.S.

Ruling that China Mobile International USA ("China Mobile") has not demonstrated that its application to provide international telecommunications services from the U.S. and foreign destinations "is in the public interest," the FCC released an order denying the application on May 10, 2019. The FCC order states that the company "is vulnerable to exploitation, influence, and control by the Chinese government" and that "in the current security environment, there is a significant risk that the Chinese government would use the [authority] to conduct activities that would seriously jeopardize the national security and law enforcement interests of the United States."

The FCC's rules afford applicants with foreign ownership from a World Trade Organization Member country such as China a rebuttable presumption that grant is in the public interest on competition grounds; however, the FCC China Mobile Order clarified that no such presumption applies to national security and law enforcement issues. Rather, these separate, independent factors are reviewed by Team Telecom, a working group of representatives from the federal government entities charged with ensuring national security—the Departments of Homeland Security, Defense, Justice, State, Treasury, and Commerce, as well as the US Trade Representative, and the FBI.

In his statement accompanying the order, FCC Chairman Ajit Pai wrote, "if this application were granted, the Chinese government could use China Mobile to exploit our telephone network to increase intelligence collection against the U.S. government agencies and other sensitive targets that depend on this network."

Conclusion

The EO sets forth the federal government's new risk-based security approach. The process will now turn to the Department of Commerce and the FCC, among others, to implement its broad terms, including identifying foreign adversaries. Per the EO, this process is to conclude no later than October 12, 2019. Meanwhile, the FCC's China Mobile Order exemplifies the new analysis—a Chinese government-controlled company cannot build a network in or provide service from the U.S. if an agency concludes that there are risks that the company would sabotage the security of other networks located in the U.S., steal personal information, engage in espionage, and/or disrupt communications services.

Angela E. Giancarlo, partner, Mayer Brown, handles a multitude of complex matters within the technology, media, and communication sector. Ms. Giancarlo counsels on the legal, business, and policy implications of proposed transactions, enforcement actions, proposed legislation and regulation, spectrum allocations for new and existing technologies and services, spectrum auctions for new and existing technologies and services, and issues related to market convergence and competition, at the FCC and globally. She is available at agiancarlo@mayerbrown.com. Ms. Giancarlo gratefully acknowledges the assistance given by her partner, Howard Waltzman, and associate attorney Timothy Lee.

