Congress of the United States
House of Representatives
SELECT COMMITTEE ON THE CHINESE COMMUNIST PARTY
548 Cannon House Office Building
Washington, D.C. 20515
(202) 225-6002

747

August 07, 2023

The Honorable Jessica Rosenworcel
Chairwoman
Federal Communications Commission
45 L St. NE
Washington, DC 20554

Dear Chairwoman Rosenworcel,

We write to request information about the security risks posed by cellular connectivity modules provided by companies subject to the jurisdiction, direction, or control of the People's Republic of China (PRC) or the Chinese Communist Party (CCP). Connectivity modules are components that enable Internet of Things (IoT) devices—from cars to medical equipment to tractors—to connect to the internet. Connectivity modules are typically controlled remotely and are the necessary link between the device and the internet.

Recent events demonstrate the power of these small modules. Last year, Russia stole $5 million worth of farm equipment from a John Deere dealership in Ukraine and attempted to bring it back to Russia.[1] Luckily, that equipment was embedded with Western-made connectivity modules. Because the modules can be controlled remotely and the vehicles require internet connectivity to operate, remotely shutting down the module allows the module provider to shut the vehicle down. When Russia moved the stolen John Deere vehicles across the border into Russia, the modules were disabled—shutting down the equipment and effectively turning the vehicles into bricks.

Connectivity modules are used in a wide variety of devices throughout the U.S., from consumer 'smart devices', to electric cars, to U.S. telecom networks regulated by the FCC.[2]

[1] Olexsandr Fylyppov and Tim Lister, *Russians plunder $5M farm vehicles from Ukraine – to find they've been remotely disabled*, CNN (May 1, 2022) https://www.cnn.com/2022/05/01/europe/russia-farm-vehicles-ukraine-disabled-melitopol-intl/index.html.
[2] Charles Parton, Comment Letter (Nov. 25, 2022), https://www.fcc.gov/ecfs/document/10509287356174/1.

Serving as the link between the device and the internet, these modules have the capacity both to brick the device and to access the data flowing from the device to the web server that runs each device. As a result, if the CCP can control the module, it may be able to effectively exfiltrate data or shut down the IoT device. This raises particularly grave concerns in the context of critical infrastructure and any type of sensitive data.

Indeed, the CCP is well aware of the importance of IoT modules. It has given extensive state support to its cellular IoT industry, led by Quectel and Fibocom.[3] Quectel provides modules to leading international firms. They are used in smart cities, drones, and U.S. first responder body cameras.[4] Fibocom, meanwhile, targets individual collaborations with major tech players.[5]

PRC law requires companies to comply with the Party's commands, including requests for data whether it is stored in the PRC or elsewhere.[6] In addition, observers have expressed concerns that both companies are closely integrated into the PRC military and state security.[7] Fibocom even states on its website that people using Fibocom's Platform "shall comply with…the laws of the People's Republic of China," which implies that Americans using a device with a Fibocom module can be surveilled pursuant to PRC law.[8]

Under your leadership, the FCC has taken important steps to counter the nefarious influence of CCP-controlled technology in U.S. telecom networks, including adding equipment and services to the Covered List from companies such as Huawei, ZTE, and Hikvision, among others.[9] Luckily, unlike in the Huawei case, there are still many U.S. and allied firms that compete with PRC cellular IoT module providers—such that restricting Quectel and Fibocom's access to the U.S. market would not undermine U.S. telecommunications networks.

Tackling PRC cellular IoT modules is a natural next step for the FCC, in consultation with appropriate national security agencies. For one, Quectel and Fibocom supply companies whose equipment is already on the FCC's Covered List.[10] The equipment on this list poses a national security threat to the U.S. and may not receive authorization for importation or sale in the U.S. Similar scrutiny should be considered for any PRC cellular IoT modules in this equipment.

---

[3] *Id.*; RUSH DOSHI, EMILY DE LA BRUYERE, & NATHAN PICARSIC, CHINA AS A 'CYBER GREAT POWER:' BEIJING'S TWO VOICES IN TELECOMMUNICATIONS (2021). For 2017–2019 figures, *see* QUECTEL, 2019 QUECTEL ANNUAL REPORT, https://www.quectel.com/wpcontent/uploads/2021/03/Quectel-Annual-Report-2019.pdf.
[4] *The World's Largest Shipments; Huawei, Alibaba and Tencent Are All Its Customers. Where is Shanghai Quectel?*, KANDIAN EXPRESS (March 12, 2020).
[5] Parton, *supra* note 2.
[6] Murray Scot Tanner, *Beijing's New National Intelligence Law: From Defense to Offense*, LAWFARE (July 20, 2017), https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense.
[7] Parton, *supra* note 2.
[8] FIBOCOM, LEGAL STATEMENT, https://www.fibocom.com/en/legalnotice/index.html.
[9] FCC, PROHIBITION ON AUTHORIZATION OF "COVERED" EQUIPMENT, https://www.fcc.gov/laboratory-division/equipment-authorization-approval-guide/equipment-authorization-system.
[10] Parton, *supra* note 2.

We respectfully request information on the PRC IoT threat. Please respond to the following questions by August 21, 2023:

1. Is the FCC, or other agencies with which it collaborates on national security issues, able to track the presence of Quectel, Fibocom, and other cellular IoT modules provided by PRC-based companies in the U.S.? Can the FCC provide further information about these modules in U.S. networks?

2. Does the FCC share our concerns about the presence of PRC cellular IoT modules in U.S. networks?

3. We understand that the FCC is considering whether to require measures to address individual component parts.[11] Is the FCC considering using the Covered List to tackle PRC cellular IoT modules? Could requiring certification for modules used in communications equipment be an effective means of countering PRC cellular IoT modules in U.S. networks? What other potential solutions exist in the view of the FCC?

4. Does the FCC require or desire further statutory authorities to combat the threat that PRC cellular IoT modules pose?

The House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party has broad authority to "investigate and submit policy recommendations on the status of the Chinese Communist Party's economic, technological, and security progress and its competition with the United States" under H. Res. 11.

To make arrangements to deliver a response, please contact Select Committee staff at (202) 226-9678.

Thank you for your attention to this important matter and prompt reply.

Sincerely,

Mike Gallagher
Chairman

Raja Krishnamoorthi
Ranking Member

[11] FCC 22-84, PARA. 282 (Nov. 11, 2022).