SEMTECH®

ABOUT THE FCC COVERED LIST

19 OCT 2023

The FCC Covered List

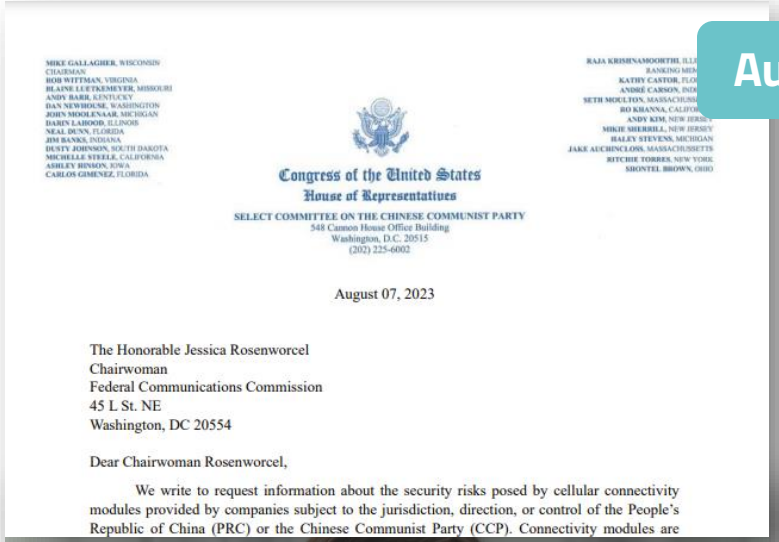
The U.S. Federal Communications Commission (FCC) first created the "Covered List" in March 2021 to describe the equipment and services that pose a national security threat.

Federal funds cannot be used to purchase equipment from companies on the Covered List, and the FCC will not authorize new equipment from companies deemed national security threats to be imported and operated in the U.S.

The Covered List (Source: FCC)

Company	Date of Inclusion on Covered List
Huawei Technologies Company	March 12, 2021
ZTE Corporation	March 12, 2021
Hytera Communications Corporation	March 12, 2021
Hangzhou Hikvision Digital Technology Company	March 12, 2021
Dahua Technology Company	March 12, 2021
AO Kaspersky Lab (a Russian company)	March 25, 2022
China Mobile International USA Inc.	March 25, 2022
China Telecom (Americas) Corp.	March 25, 2022
Pacific Networks Corp and its wholly-owned subsidiary **ComNet (USA) LLC**	September 20, 2022
China Unicom (Americas) Operations Limited	September 20, 2022

FCC Urged Inclusion of Quectel and Fibocom in the Covered List



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

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

August 7, 2023

Two U.S. Representatives (Mike Gallagher and Raja Krishnamoorthi) submitted a letter to Jessica Rosenworcel, the chairwoman of the FCC, raising their concerns about "the **potential national security risks posed by certain Chinese-manufactured cellular Internet of Things (IoT) modules**...",

"We are particularly concerned about two companies, **Quectel** Wireless Solutions Co., Ltd. (Quectel) and **Fibocom** Wireless Inc. (Fibocom)..."

"PRC (People's Republic of China) law requires companies to comply with the Party's commands, including **requests for data whether it is stored in the PRC or elsewhere**."

See the original letter from Select Committee on the CCP

September 5

FCC Chairwoman Jessica Rosenworcel asked U.S. government agencies to consider declaring that Chinese companies including **Quectel and Fibocom Wireless pose unacceptable national security risks**.

She said, "FCC welcomes the opportunity to collaborate "in addressing this threat, including **consideration of the inclusion of this equipment (cellular IoT modules) from Quectel and Fibocom on the Covered List**."

Source: Reuters

What Does it Mean to Enterprises Using IoT Modules?

If the FCC includes the 2 Chinese module vendors in the Covered List, it could have several impacts on their users:

- **Disruption of Supply Chain**: The addition of these companies to the Covered List may disrupt the supply chains of businesses that rely on their products. This could potentially lead to product shortages or delays.

- **Increased Costs:** Businesses may need to find alternative suppliers and potentially redesign their products, resulting in increased costs and delays.

- **Regulatory Compliance Challenges:** Companies using the covered products would need to recertify their products to ensure ongoing compliance with FCC regulations. This could require a significant investment of time (months) and resources (thinking $50k+).

Recommendation

To mitigate potential business disruptions, enterprises operating in or exporting to the U.S. should prioritize the use of IoT modules from American or Western suppliers that adhere to rigorous security and data integrity standards.

Why Sierra Wireless (Semtech) is your best choice of IoT module supplier?

1.Uncompromised Integrity: Since our establishment in 1993, Sierra Wireless has proudly been headquartered in Canada, a country renowned for its robust privacy laws and constitutional protections that limit government access to personal information. This commitment to privacy is further reinforced by our integration into Semtech, a reputable U.S. semiconductor company. Our customers can place complete trust in our secure supply chain and unwavering commitment to data integrity, especially for critical infrastructure deployments.

2.Regulatory Compliance: As a North American company, we are fully committed to upholding all relevant regulations. Our dedication to compliance ensures that we do not utilize any products or services from the FCC Covered List. By choosing our IoT modules, enterprises can avoid the risk of having to modify their designs due to regulatory concerns.

3.Longevity and Reliability: With 30 years of experience in the IoT industry, Sierra Wireless remains a pioneer, a trustworthy IoT partner to our customers. Our IoT modules have earned a well-deserved reputation for exceptional reliability. Our customers can confidently rely on our modules, as well as our experienced engineering and support teams, knowing that their IoT applications will be seamlessly connected, providing them with peace of mind.

SEMTECH