Most Immediate ***Ref: ITU-APT/L/2022-2023/777***

August 11, 2023

To

Shri S. Jaishankar,
Hon'ble Minister of External Affairs of India
South Block
New Delhi-110001

Dear Sir,

Greetings from the ITU-APT Foundation of India (IAFI) a non-profit, nonpolitical registered society in India, supporting Indian private sector participation in the activities of International Telecommunications Union (ITU), the specialized UN agency for ICT.

Every 4 years, ITU organizes a global conference called "World Radio Conference" to update the Radio Regulations which is an international legal treaty on the use of Radio spectrum.

This year WRC-23 will be held in Dubai from 20 November to 15 December 2023. For this conference China is pushing to allocate the 6 GHz band for mobile services along the EMEA (BRI) corridor to promote their control over this territory. In this connection, please see enclosed letter to the FCC chairman. Most countries in the world have already allocated the Lower 6GHz (5925-6425 MHz) band for WiFi, and many developed countries including USA (and the QUAD) have also allocated the upper GHz band for Wi-FI.

The 6th Meeting of the Conference Preparatory Group for WRC-23 (APG-6) will be held at Brisbane, Australia from 14th to 19th of August 2023 to finalize the Preliminary APT Common Proposals (PACPs). This will be the final APG meeting before WRC-23. China is pushing the Asian countries for a pro-China stand and will be meeting with the Indian Government head of delegation at that meeting and seeking support for their proposal. We believe this proposal is not in the national interest of India.

In India, we generally follow the ITU Radio Regulations. So far ITU has not decided about the use of the upper 6 GHz spectrum band for the purpose of Mobile services. Currently the WRC-23 conference, is expected to consider the upper band for 5G in Europe, Middle East and African Region – known as ITU Region 1. The proposal for the Asia Pacific -ITU Region 3 – was earlier rejected by the previous WRC-19 at the instance of India due to likely negative impact on our satellite services but China is asking for a relook into that decision.

Delicensing of the lower 6GHz band would enable roll out of AR/VR/MR devices and new applications & services in the areas of healthcare, education, etc. all of which are running on Wi-fi 6E. Public WiFi, which is a national priority, will further enable delicensing of the 6 GHz band to meet the countries' socio-economic needs. A short note on the issue is enclosed.

We request MEA to provide suitable guidance to the Indian delegation going to Australia this week to deal with this Chinese initiative, which we belive is not in India's national interest.

Bharat B Bhatia,
President, ITU-APT Foundation of India (IAFI)
Vice Chairman, Asia Pacific, World Wireless Research Forum(WWRF)

Copy to :

1. ***Shri Ashwini Vaishnaw,***
   Hon'ble Minister of Communications and IT
   Sanchar Bhawan
   New Delhi-110001
2. ***Secretary, Department of Telecommunications***
   Sanchar Bhawan
   New Delhi-110001
   (Kind Attn. Wireless Advisor to the Government of India)

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 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 nefariousinfluence 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 competewith 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

We respectfully request information on the PRC IoT threat. Please respond to the followingquestions 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 addressindividual component parts.[11] Is the FCC considering using the Covered List to tackle PRCcellular 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 PRCcellular IoT modules pose?

The House Select Committee on the Strategic Competition Between the United States andthe 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).

Note for Delicensing of 6GHz band

Wi-Fi Data traffic has been growing at a much faster rate with the rollout of 5G. This has been the case with each successive cellular generation from 2G onwards. Demand for Wi-Fi will only continue to grow with increased fiber deployments and cellular generations. Next generation use cases will require much faster data to enable immersive experiences such as robotic surgeries, Industrial automation, AR/VR. This requires expansive computational resources and connectivity- several times faster than 5G. Such high speed cannot be delivered by a wide-area networks such as IMT. Instead, local-area, short range communications such as the next generation Wi-Fi technologies designed for extremely high throughput and spectral reuse is the only solution. Wi-Fi 6E has the capabilities required for advanced use cases as it delivers faster speed, lower latency, higher efficiency, and higher density. It is a success already and by 2024 there will be billions of devices installed globally, able to operate from 5.925 to 7.125 GHz, from over 1.5 million Wi-Fi 6E access points and 350 million Wi-Fi 6E devices in 2022. 6 GHz frequency band is uniquely suited to meet growing demand for Wi-Fi, connectivity. There is no alternative spectrum now or in the future.

IMT networks in 6 GHz are not feasible as frequency harmonization cannot be achieved as most countries in the world have already opened this band for Wi-Fi. Besides, market fragmentation does not allow economies of scale necessary for a viable IMT ecosystem in 6 GHz. Wi-Fi 6E in 6 GHz band has expanded significantly around the world since 2020. More than 40 countries such as USA, Australia, Hong Kong, Japan, Malaysia, European Union, Norway, Switzerland, UK, Jordan, Morocco, Qatar, UAE etc. have already adopted it while several other countries are considering the 6 GHz band for part or full for license exempt use. Wi-Fi 7 and Wi-Fi 8 that enables enhanced VR/AR/XR, Industrial IoT, automotive, telepresence, immersive 3-D will depend on the 6 GHz access, and 320 MHz channels will be optimized for demanding emerging use cases.

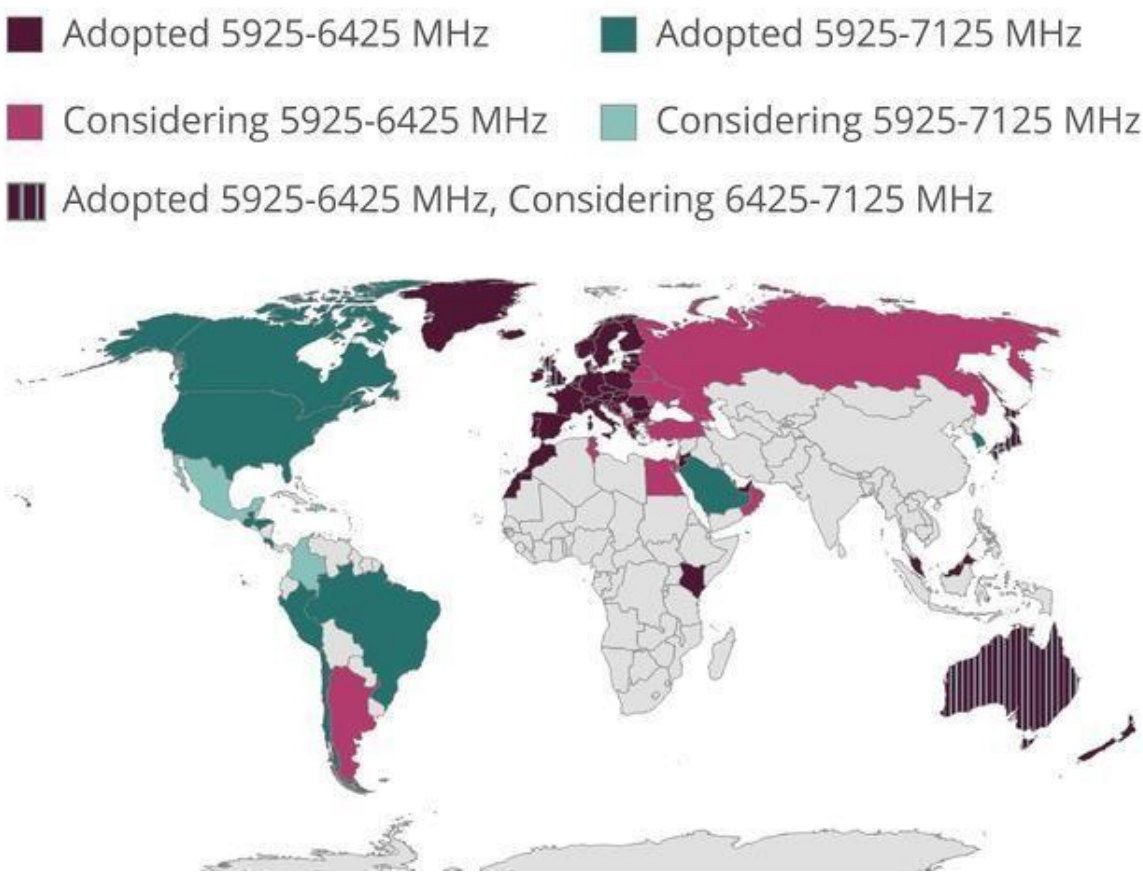
IAF has been building momentum with other industry stake holders to open the 6GHz frequency bands for a license exempt use in India and other Asian Countries. Eralier, I met with Shri K. Rajaraman, Secretary DoT and made a presentation on this issue as a part of the outcome of our recent spectrum conference. The 2nd India Spectrum Management Conference that was inaugurated by Hon'ble Minister of State for Communications, Shri Devusinh Chauhan.

License exempt use of 6GHz will open new opportunities for innovators and manufacturers to develop products and technologies and also increase opportunities for smart home and industrial products being manufactured in India for export markets. 6 GHz band is currently extensively used by

satellites for up linking of broadcasting channels as well as by VSAT for providing data connectivity. Therefore, it will not be possible to use this band for licensed mobile operators. However, as various studies have shown, this band could be shared by indoor-only low-power Wi-fi routers. Since the band cannot be auctioned, delicensing it for Low Power indoor use will not cause any revenue loss to the Government. On the other hand, this move will add huge economic benefit to the economy and help increase the GDP. In addition, this move will also support, Atamnirbhar India as most of the Wi-Fi routers are fully made in the country.

We therefore humbly request you to kindly open the 6 GHz band for license exempt use of WiFi urgently so that software and hardware exporters in India could access this huge global market.

Countries that have adopted the new Wi-Fi 6E / 6 GHz frequency spectrum?



Source: Wi-Fi Alliance | Nations Adopting Wi-Fi 6E / 6 GHz

Much of North and South America have fully implemented Wi-Fi 6E / 6 GHz. The following countries have fully begun commercial utilization of the 5925-7125 MHz frequency space:

- Brazil
- Canada

- Costa Rica
- Guatemala
- Honduras
- Peru
- Saudi Arabia
- United States

Many more countries have adopted, 5925-6425 MHz:

- Australia
- Chile
- European Union
- Hong Kong
- Iceland
- Japan
- Jordan
- Kenya
- Liechtenstein
- Malaysia
- Morocco
- New Zealand
- Norway
- Qatar
- Switzerland
- United Arab Emirates
- United Kingdom

Of these nations, Japan, Qatar, and the United Kingdom are considering use of the higher end of the Wi-Fi 6E / 6 GHz frequency space, 6245-7125 MHz

The following nations are considering use of the full Wi-Fi 6E / 6 GHz frequency spectrum, 5925-7125 MHz:

- Australia
- Colombia
- Hong Kong
- Mexico