

United States Senate

WASHINGTON, DC 20510-0908

June 18, 2026

The Honorable Brendan Carr
Chairman
Federal Communications Commission
45 L Street NE
Washington, D.C. 20554

Dear Chairman Carr:

We write to request that the Federal Communications Commission (FCC) provide a briefing to members and staff of the U.S. Senate Special Committee on Aging on the national security risks posed by foreign adversary-manufactured modular transmitters embedded within health wearable devices marketed and sold in the United States. As the Chinese Communist Party (CCP) intensifies its campaign to steal and exploit private consumer data, we have a solemn obligation to ensure that the health devices our nation's seniors depend on daily do not expose them to unacceptable security risks.

The FCC's Second Report and Order of October 28, 2025, confirmed that People's Republic of China (PRC)-origin modular transmitters embedded within consumer devices, including health wearables, merit scrutiny even when the finished goods manufacturer isn't based in an adversarial nation (i.e. Communist China). Every smartwatch, fitness band, remote patient monitor, and personal emergency response device that transmits data wirelessly likely does so through a modular transmitter subject to the Commission's equipment authorization rules under 47 CFR § 15.212(a).¹

One of China's dominant cellular Internet of Things (IoT) manufacturers, Quectel, was recently added to the Section 1260H list of Chinese Military Companies maintained by the Department of Defense.² While consumers, including seniors, believe that their health wearables may be completely secure, the unfortunate reality indicates that in all likelihood, the most intimate details of their health may be accessible by a foreign adversarial government. In fact, only three of the top 10 IoT global module manufacturers are insulated from the Chinese Communist Party, and one of those three exited the IoT module market last year.³ In the PRC's case, their domestic cybersecurity law compels companies to provide access to their data and technology to the central government upon demand⁴, which means that every device sold by a PRC-based wearable manufacturer, and any

¹ [54B9433A-2DB2-4567-92C2-6B236364A9EF](#) (Letter to Chairman Carr from Senator Rick Scott and Congressman Andy Ogles, 17 DEC 2025).

² <https://media.defense.gov/2025/Jan/07/2003625471/-1/-1/1/ENTITIES-IDENTIFIED-AS-CHINESE-MILITARY-COMPANIES-OPERATING-IN-THE-UNITED-STATES.PDF>

³ <https://libertybellproject.us/reports/spies-saboteurs-and-access-to-u-s-connected-devices/>

⁴ https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf

sensitive personally identifiable information (PII) is potentially accessible to Beijing, with or without the user's knowledge or consent.

Incidentally, the global market for consumer health wearables themselves is also dominated, in terms of unit volume and price point, by manufacturers based in the PRC. Modern connected health wearables continuously monitor several critical health indicators, including heart rate, blood pressure, blood oxygen saturation, electrocardiographic activity, sleep, body temperature, and blood glucose levels.⁵ These biometric parameters are directly relevant to intelligence about an individual's physical vulnerabilities, and, in aggregate, provides population level health profiles that could be used to train artificial intelligence (AI) models for non-civilian applications.

By 2027, worldwide wearable shipments, which includes smartwatches, fitness trackers, and connected health monitors, are projected to grow to 625.4 million units⁶, a figure boosted in part by low-cost Chinese-manufactured devices.⁷ While many Chinese health wearable devices are not yet widely available in the United States, many Chinese companies are expected to submit competitive bidding applications to the Centers for Medicare and Medicaid Services, risking a flood of U.S.-bound products in the coming years. Some Chinese health wearables manufacturers already continue to distribute their products throughout the U.S. consumer market, including Xiaomi (especially through its affiliate, Zepp Health) and even select products of Covered List-sanctioned Huawei.⁸ These two companies were found in a June 2025 peer reviewed study published in *npj Digital Medicine* to have the highest cumulative privacy risk scores of any wearable manufacturer in a 17-company, 24-criteria analysis.⁹ Of all companies assessed in this study, Xiaomi achieved the highest risk score of 60 out of a possible 72, with 16 out of 24 criteria rated as "High Risk." Huawei received 14 High Risk ratings.

While the threat of Chinese health wearable data exfiltration affects all Americans, we are especially concerned about the risk to senior citizens who increasingly rely on specific categories of connected health monitoring devices primarily designed and marketed for their use. These products, enumerated below, can collect highly sensitive, medically actionable information that goes far beyond what a typical consumer fitness tracker captures. They are, in many cases, the very devices that determine whether a senior receives emergency medical care, whether their medication is working, and whether they are safe to remain in their own home.

In anticipation of a briefing to the U.S. Senate Special Committee on Aging, we respectfully request that the Commission review the following categories of connected

⁵ <https://www.nature.com/articles/s44325-025-00082-6>

⁶ <https://www.businesswire.com/news/home/20230920033505/en/Wearables-Bounce-Back-with-8.5-Growth-in-Q2-2023-and-a-Positive-Forecast-According-to-IDC>

⁷ Ibid

⁸ [Amazon - Huawei Watch](#)

⁹ <https://www.nature.com/articles/s41746-025-01757-1>

health products, as well as any foreign adversary-manufactured modular transmitters used in these products, for data security and privacy risks. We further request an assessment of whether these risks may warrant inclusion of such products and transmitters on the Covered List on a going-forward basis.

1. Personal Emergency Response Systems (PERS) and Fall Detection Wearables

Personal emergency response systems, including those worn on the wrist or as a pendant, are critical for senior independent living. They collect GPS location data, fall detection data, and critical physiological data. An unknown but significant share of the cellular modules within PERS devices – even those sold under American brand names – may originate from industry scale PRC-based suppliers, including Quectel and Fibocom.¹⁰¹¹ Any PERS device whose modular transmitter or embedded processor originates from a PRC-based company not yet on the Covered List may still represent a direct pathway for data exfiltration or remote disruption.

2. Smartwatches and Fitness Trackers

Health wearables sold by PRC-based companies warrant serious scrutiny over how they handle user data. Amazfit, which markets smartwatches and fitness trackers in the United States through its parent company Zepp Health, has clear historical and organizational ties to Xiaomi¹², one of China's largest and most politically connected technology firms.¹³ In 2020, researchers reportedly found that Xiaomi was monitoring the phone activity of millions of people, raising considerable consumer data privacy concerns.¹⁴

3. Remote Blood Pressure and Cardiac Monitors

Andon Health, a PRC-based company¹⁵ operating in the United States under its subsidiary iHealth Inc.¹⁶, manufactures FDA-approved¹⁷ blood pressure monitors and digital thermometers. Because these devices capture sensitive cardiovascular and metabolic data and transmit it to cloud platforms, they present exactly the kind of risk members of Congress have previously¹⁸ identified with respect to genetic sequencing devices connecting to research networks and cloud services.

¹⁰ *ibid*

¹¹ <https://judiciary.house.gov/committee-activity/hearings/ip-and-strategic-competition-china-part-iv-patents-standards-and-o>

¹² <https://www.firstpost.com/tech/news-analysis/xiaomi-unveils-amazfit-smartwatch-3687679.html>

¹³ [Amazfit Smart Watch \(Amazon.com\)](https://www.amazon.com/Amazfit-Smart-Watch)

¹⁴ <https://www.forbes.com/sites/thomasbrewster/2020/04/30/exclusive-warning-over-chinese-mobile-giant-xiaomi-recording-millions-of-peoples-private-web-and-phone-use/#7f4c67bf1b2a>

¹⁵ <https://www.jiuan.com/EN/aboutUs.html?index=>

¹⁶ <https://www.prnewswire.com/news-releases/ihealth-raises-25-million-to-fuel-growth-and-global-market-share-275809751.html>

¹⁷ [iHealth Labs: FDA Approval of Wireless Blood Pressure Monitors](https://www.fda.gov/medical-devices/implants-and-medical-electronics/ihealth-labs-fda-approval-of-wireless-blood-pressure-monitors)

¹⁸ See footnote 1

4. Continuous Glucose Monitors and Metabolic Wearables

Continuous glucose monitors, which transmit real-time blood sugar data to smartphones and cloud platforms, are life critical devices for millions of seniors living with Type 2 diabetes. For seniors living with this chronic disease, that data stream constitutes the disclosure of medication adherence, dietary behavior, metabolic stress, and the timing of acute health incidents. While several American companies have taken important measures to protect PII – and should be praised for doing so – it is nevertheless relevant for Congress to learn if any domestically sold CGMs and related health wearables contain embedded modular transmitters from Communist China, and what the implications may be for data privacy and national security.

5. Smart Hearing Aids and Auditory Health Devices

The U.S. Senate Special Committee on Aging further encourages the Commission to consider any risks to data privacy to our nation's seniors concurrent with the use of smart hearing aids. One in three people sixty years of age and above have hearing loss; that figure increases to between 40 and 50 percent for adults between the ages of 65-75, and 50% for seniors older than 85 years old.¹⁹ Critically, the Food and Drug Administration's approval in October 2022 of a regulatory category for over the counter hearing aids has dramatically accelerated access, to the point that PRC-based manufacturers have become significant producers of OTC hearing aids exported to the United States. Communist Chinese companies (including Huizhou Jinghao Medical Technology) manufacture Bluetooth enabled hearing aids sold under retail and white label brands in U.S. market and online channels, with little disclosure to end consumers of their origin or data governance practices. These particular products pose a clear need for increased scrutiny: former Director of National Intelligence James Clapper required a security waiver specifically because of the surveillance risk posed by his wireless enabled hearing aid.²⁰

6. Home-Based Remote Patient Monitoring (RPM) Devices

Several RPM device manufacturers, while operating in the U.S., rely on infrastructure or cloud services hosted in China, meaning that personal health data including glucose levels may be transmitted overseas, sometimes without the knowledge of patients or providers.²¹ Perhaps the most consequential example to date involves the Contec CMS8000, a patient monitor manufactured by Contec Medical Systems²², headquartered in Qinhuaogdao, China. In January 2025, CISA released a fact sheet detailing that analysts discovered an embedded backdoor function with a hard-coded IP address and functionality

¹⁹ <https://www.audiology.org/consumers-and-patients/seniors-hearing-loss/>

²⁰ <https://www.cnn.com/2016/05/18/politics/hearing-aids-clapper-security-waiver>

²¹ <https://www.businesswire.com/news/home/20250529680608/en/Smart-Meter-Highlights-Security-Risks-of-Remote-Patient-Monitoring-Devices-Sending-Patient-Data-to-China>

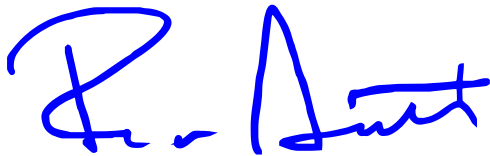
²² [Cybersecurity Vulnerabilities with Certain Patient Monitors from Contec and Epsimed: FDA Safety Communication | FDA](#)

The Honorable Brendan Carr
June 18, 2026
Page Five

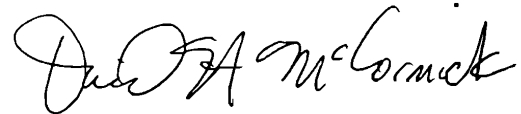
that enables patient data spillage exists in all firmware versions analyzed.²³ The U.S. government warned that Chinese-made patient monitors in America were sending sensitive data back to internet locations in China, and the devices contained embedded backdoors that could allow alteration of patient data.²⁴

Health wearables are extraordinarily helpful and necessary tools in improving the quality of life for America's seniors. As a result, these life-saving products must be secured from the malign influences of foreign adversaries – our seniors deserve to know that the products they depend on are not undermining their privacy concerns. We look forward to working with the Commission on fulfilling our request for a briefing and respectfully request a response by **COB July 15, 2026**.

Sincerely,



Rick Scott
United States Senator



David McCormick
United States Senator

cc: The Honorable Robert F. Kennedy, Jr., Secretary, Department of Health and Human Services
The Honorable Mehmet Oz, Administrator, Centers for Medicare and Medicaid Services

²³ <https://www.cisa.gov/news-events/alerts/2025/01/30/cisa-releases-fact-sheet-detailing-embedded-backdoor-function-contec-cms8000-firmware>

²⁴ <https://www.fdd.org/analysis/2026/04/06/new-standards-aim-to-protect-medical-patients-from-the-internet-of-things/>