

U.S. Rep. Gallagher: Introduces bipartisan legislation to protect American networks

Posted on Monday, Nov 6, 2023

>> **WisPolitics is now on the State Affairs network. Get custom keyword notifications, bill tracking and all WisPolitics content. [Get the app or access via desktop.](#)**

WASHINGTON, D.C. — Reps. Mike Gallagher (R-WI), Ashley Hinson (R-IA), Raja Krishnamoorthi (D-IL), John Moolenaar (R-MI), Brittney Pettersen (D-CO), and Chrissy Houlahan (D-PA) introduced the [Defend our Networks Act](#). The bipartisan bill would use unobligated COVID-19 funds to replace Chinese-made telecommunications products with secure equipment to ensure Americans have reliable and private connectivity.

In a [Fox News article](#) announcing the legislation's introduction, it is estimated that there are roughly 24,000 pieces of Chinese-made communications equipment embedded in U.S. networks. Discarding this compromised equipment is critical to protecting Americans' privacy, as well as our national security, from CCP spying.

"The COVID-19 pandemic is over, but the threats posed by Chinese telecommunications companies like Huawei and ZTE are not. There are thousands of pieces of risky Chinese telecommunications equipment in U.S. networks and it's imperative we act with a sense of urgency to remove them," **said Rep. Gallagher.** *"The bipartisan Defend Our Networks Act is a common-sense way to protect Americans from national security risks in our telecom networks and ensure small telecom providers have the resources they need to replace this dangerous equipment."*

"Chinese technology is embedded in communications networks across the United States, giving the Chinese Communist Party backdoor access to Americans' personal information and sensitive data. If communication flows through Huawei or ZTE equipment, it should be treated as if it is being downloaded back to a server in

Beijing with a full access pass for the CCP regime. The Defend Our Networks Act will ensure compromised Chinese telecom equipment is replaced with secure systems so that Americans, especially those in rural areas, have secure, reliable, and private connectivity,” **said Rep. Hinson.**

“I’m proud to my colleagues in introducing the bipartisan Defend Our Networks Act to safeguard our communications infrastructure from potential vulnerabilities to the Chinese Communist Party (CCP),” **said Rep. Krishnamoorthi.** *“Communications equipment produced by companies under the influence of the CCP pose a serious risk to our national security, and fully funding efforts to replace the vulnerable components with secure ones is a vital step forward in safeguarding our technological infrastructure.”*

“This year, the Federal Communications Commission said they can only cover less than half of the costs to remove dangerous Chinese technology from American telecommunications networks. That is simply unacceptable. I am proud to co-lead the Defend Our Networks Act alongside a strong coalition of bipartisan partners. This bill would strengthen the FCC’s ability to safeguard our technology, ensuring that Americans can be confident, knowing that none of our telecommunications systems are vulnerable to attacks because they contain Chinese software,” **said Rep. Houlihan.**

“Chinese-supplied equipment can pose security risks to our nation’s communications infrastructure. The FCC has now banned the purchase of this equipment, which is why we must invest to replace the older equipment still being used. I’m joining my colleagues in introducing this bipartisan bill to protect rural wireless networks and defend our country against national security threats,” **said Rep. Pettersen.**

Read the bill text [HERE](#).

Background:

Due to their close ties to the Chinese government, Huawei and ZTE equipment presents significant risks to U.S. national security and domestic communications networks. The Federal Communications Commission (FCC) has already prohibited the purchase of Huawei and ZTE products and banned the use of FCC funds to expand or maintain networks containing any Huawei or ZTE equipment, and ordered telecom carriers to tear out telecom equipment made by

Huawei and ZTE. However, this equipment is still embedded throughout U.S. networks.

In 2020, Congress passed the bipartisan Secure and Trusted Communications Networks Act, which created the Secure and Trusted Communications Networks Reimbursement Program at the FCC. Also known as the Rip and Replace program, this effort reimburses smaller communications providers for costs associated with removing, replacing, and disposing of this at-risk equipment. However, the FCC confirmed that the program faces a \$3.08 billion shortfall. This shortfall means carriers will continue using compromised equipment or “rip and not replace,” leaving Americans without communications service. This would disproportionately impact rural areas, where many communities only have one carrier, leading to a loss of service.