

**STATEMENT OF  
COMMISSIONER MICHAEL O'RIELLY**

Re: *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89.

Maintaining the security and integrity of our communications infrastructure is of paramount importance. Over the past year or so, it rightfully has been a heightened priority of the FCC, Administration, and Congress to protect our communications networks from external threats, such as incursions by the Chinese Communist government through the “companies” they control.

For instance, the Commission prohibited certain equipment from being supported by Universal Service Funds, designated Huawei and ZTE as potential threats to our infrastructure, and sought comment on ripping and replacing certain equipment from all networks, among other actions. The President has signed an executive order providing the Department of Commerce with the authority to prohibit transactions when they would pose a threat to U.S. infrastructure or national security. Congress has passed multiple bills addressing Huawei and ZTE and created the Federal Acquisition Security Council to lead a government-wide effort to evaluate threats posed by communications services and equipment. Most recently, the Secure 5G and Beyond Act, authored by Senators Cornyn, Burr, and Warner, was signed into law to keep 5G networks secure from foreign interference. I appreciate that all of these efforts have brought added attention to and provided much needed guidance on these important issues.

Most relevant to today’s item is the Secure and Trusted Communications Networks Act, which incorporates and expands upon the 2019 actions taken by the Commission. The item declares that the FCC’s actions to prohibit USF funds from being spent on Huawei and ZTE equipment is consistent with and satisfies certain provisions of the Act, and it seeks comment on how to implement the remainder of the law. As always, I will follow Congressional direction and fully support our action today. Many thanks to Representatives Pallone, Walden, Matsui, and Guthrie, along with Senators Wicker, Thune, Cotton, Warner, Markey, and Sullivan, for ushering this bill through Congress.

I do have one area of concern, however, that is related to today’s item. With all of the activity previously described, there are multiple conversations taking place about what equipment and services pose an actual risk to our national security. This is an important, but not easy, undertaking and involves some necessary line drawing. The FCC used a very broad definition in 2019, and, based on our definition, certain entities reported to the FCC whether they had covered equipment in their networks. Other federal agencies, however, do not appear to be taking the exact same approach. Given the lack of consensus on what equipment and services pose a national security risk, we should take a step back and delay any publication of the list of companies that reported covered equipment under our definition.

Publicly exposing companies, which did not do anything wrong at the time they purchased their equipment, and potentially causing substantial financial harm should only be considered as a necessary step if their equipment is ultimately determined to pose a true threat. This is not to say that the Commission erred in requesting this data, as sometimes there is a first mover disadvantage, or that this information does not provide the Commission with useful insights. But, in order to provide certainty to industry and clarity to Americans about the actual risks of using certain networks, all involved federal agencies should be on the same page regarding what equipment and services could harm our national security before prematurely publishing a list of names, which, in the end, may include companies whose equipment ultimately is determined not to cause concern.

I thank the Chairman for bringing this important item to a vote. I approve.