wiley

ALERT

FCC Acts on National Security, Signaling Future Regulatory Interests

November 27, 2019

On November 22, 2019, the Federal Communications Commission (FCC or Commission) took action to address what Chairman Ajit Pai considers dangerous Chinese influence in the nation's communications networks. Its proceeding, *Protecting National Security Through FCC Programs,* heralds a new approach to oversight of the nation's telecom networks. In the items voted on:

- The Commission prohibits the use of Universal Service Funds (USF) by carriers to purchase equipment and services from companies that the FCC determines pose a national security threat, effective immediately upon publication in the Federal Register. It further mandates information collection and auditing obligations that will affect recipients of USF program funding.
- The Commission also kicks off another regulatory proceeding to look at whether to require carriers receiving USF funds, known as eligible telecommunications carriers, to remove and replace existing equipment and services from covered companies.
- Additionally, as part of its information collection efforts, the Commission voted to expand the scope of the Further Notice of Proposed Rulemaking (FNPRM) "beyond the initial proposal, which focused on removing equipment if the carrier receives federal support, to asking whether [the Commission] should mandate the removal of covered equipment regardless of whether the communications provider receives federal support," as noted in the Statement of Commissioner Carr.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Edgar Class
Partner
202.719.7504
eclass@wiley.law

Kevin G. Rupy
Partner
202.719.4510
krupy@wiley.law

Practice Areas

Government Contracts
International Trade
National Security
Privacy, Cyber & Data Governance
Telecom, Media & Technology

The FCC's vote increases regulatory risk for the private sector and confirms the expanding federal interest in supply chain and business operations across the information and communications technology sectors. It comes amidst an array of federal activities on telecom and Internet security, supply chain, trade, and global standards that will affect emerging technologies like the Internet of Things. This alert explains the item and provides important context and indications about the future of FCC activity in this area.

Report and Order

The item adopts a rule that no universal service support may be used to purchase or obtain any equipment or services produced or provided by a covered company posing a national security threat to communications networks or the communications supply chain. As a basis of authority, the FCC relies on Section 254 of the Communications Act, which permits placing reasonable public-interest conditions (such as national security) on the use of USF funds. The agency also cites to Section 201(b) of the Act and Section 105 of the Communications Assistance for Law Enforcement Act (CALEA) as a basis for its authority.

The Report and Order initially designates Huawei Technologies Company and ZTE Corp. as companies covered by the rule, and provides separate justifications for each company's designation. The FCC concludes that both companies pose a "unique threat" to network and supply chain security due to their size, close ties to the Chinese government, security flaws in their equipment, and the "unique end-to-end nature of Huawei's service agreements that allow it key access to exploit for malicious purposes." It also points to the Chinese government's broad authority to compel support and assistance to its intelligence agencies, which the FCC concludes is "particularly troublesome, given the Chinese government's involvement in computer intrusions and attacks as well as economic espionage."

The FCC also establishes a process for designating additional covered companies in the future. The process includes a public notice and comment period for initial determinations that a company poses a national security threat to communications networks or the supply chain. Such initial determinations can be made either *sua sponte* by the FCC, or in response to a petition from an outside party. If an initial designation is unopposed, the entity shall be deemed to pose a national security threat 31 days after the issuance of the notice. If any party opposes the initial designation, the designation is subject to a more robust administrative framework, and shall take effect only if the FCC determines that the affected entity should be designated as a covered company.

The Order prohibits the future use of USF funds to purchase equipment or services from covered companies, to include upgrades to existing equipment and services. USF recipients must be able to affirmatively demonstrate that they have not used any funds obtained via the USF to purchase, obtain, maintain, improve, modify, or otherwise support any equipment or services provided or manufactured by a covered company. Although the FCC states that its rule does not prohibit USF recipients from using their own funds to purchase or obtain equipment or services from covered companies, USF recipients must be able to clearly demonstrate that is the case.

Finally, the FCC also establishes a certification and audit regime to enforce the new rule. The agency directs the Wireline Competition Bureau, in coordination with the Universal Service Administrative Company (USAC), to revise the relevant information collections for each of the four USF programs to require a certification attesting to such compliance. USAC is also directed to implement audit procedures for each program consistent with the new rules.

Further Notice of Proposed Rulemaking

In an accompanying FNPRM, the FCC proposes to require eligible telecommunications carriers receiving USF support to "remove and replace" existing equipment and services from covered companies. The FCC, however, proposes to make any such requirement contingent on the availability of a funded reimbursement program. The FNPRM also seeks comment on expanding the scope of its rules beyond eligible telecommunications carriers. First, it seeks comment on whether to expand its proposed removal and replacement requirement to all USF recipients, rather than limit it to only eligible telecommunications carriers (ETCs). Second, the FCC also asks whether it "can and should" prohibit *any* communications company from purchasing, obtaining, or otherwise supporting any equipment or services produced or provided by a covered company, regardless of whether they use USF funding to do so. Should the FCC expand its prohibition more broadly, it also seeks comment on whether companies replacing such equipment should be included in any reimbursement program.

The FNPRM also seeks comment on how to pay for such removal and replacement. Among other things, it seeks comment on determining the reasonableness of costs associated with replacement of products and services, and what types of restrictions it should place on such expenses. The FCC also seeks comment on its proposal to seek funding from Congress for the removal and replacement of covered equipment, and the appropriate level of any such funding request. Absent Congressional funding, the FCC seeks comment on using USF funding to provide support for replacing existing equipment and services.

Information Collection Order

To help the FCC design this program for removal and replacement "the FCC will conduct an information collection to determine the extent to which eligible telecommunications carriers have equipment from Huawei and ZTE in their networks and the costs associated with removing and replacing such equipment." The agency directs the Wireline Competition Bureau (WCB) and Office of Economics and Analytics (OEA), in coordination with USAC, to conduct the information collection.

WCB and OEA are directed to collect information from eligible telecommunications carriers as to whether they own equipment or services from Huawei or ZTE, what that equipment is and what those services are, the cost to purchase and/or install such equipment or services, and the cost to remove and replace such equipment or services. The information collection is currently limited only to eligible telecommunications carriers, although the FCC will permit some service providers to participate voluntarily (such as those with pending eligible telecommunications carrier designation petitions, and other USF recipients who are not ETCs). WCB and OEA are directed by the FCC to "proceed expeditiously" with the information collection, including by seeking

emergency Paperwork Reduction Act approval from the Office of Management and Budget.

Compliance Challenges Loom

Eligible telecommunications carriers and USF recipients will have to think about their supply chains and how they plan to comply with new restrictions and obligations, as well as consider how to seek any available funding for removal and replacement of existing covered equipment. Federal funds may be made available by Congress or the FCC, but any receipt of federal funds comes with strings attached. One such string is the possibility of audit and enforcement action, long a staple of FCC and USAC. In our extensive experience before the FCC and USAC, such proceedings can be complex and burdensome, and can lead to collateral proceedings under the False Claims Act.

Likewise, compliance with information collection requirements require care and planning. Companies subject to information collection mandates should consider their responses and their confidentiality. The FCC has mechanisms to protect submitted information, which should be considered.

The Broader Context

The United States is in the midst of several overlapping and interrelated efforts on telecom and internet security, including 5G. Senate leadership has called for a coordinated national plan and Administration leader on 5G security. Security issues are being addressed in several Executive branch actions, including a May Executive Order on Securing the Information and Communications Technology and Services Supply Chain (EO), the recently released rules implementing the EO, and the placement by the Department of Commerce's Bureau of Industry and Security (BIS) of Huawei and 114 of its affiliates on BIS's Entity List, severely limiting U.S. companies' ability to transact with the company.

Expect More FCC Activity and a Debate over the FCC's Approach

Each Commissioner weighed in on the items and the future of FCC activity. Collectively, they signal a vigorous future for national security at the FCC.

Chairman Pai referred to serious concerns raised by Attorney General Bill Barr in a letter filed with the FCC about foreign influence in communications networks. Chairman Pai stated that protecting the networks, rural and urban alike, is a vital national security issue. He noted close ties of Huawei and ZTE to China's government and military apparatus

Commissioner O'Rielly agreed that USF dollars should not be used to support entities that intend to do us harm but also noted reservations that the FCC is "broadly and unnecessarily interpreting some statutory provisions to justify [its] authority to decide that some companies should not be able to participate in our communications economy."

Commissioner Carr discussed concerns about communications infrastructure containing Huawei equipment near military installations. He has earlier called for reopening a national security review of certain Chinese 214 license holders. Commissioner Carr stated that if equipment poses a threat, it is not enough to stop

subsidizing it—he urged mandatory removal and lauded Commissioner Starks' leadership with the "Find It, Fix It, Fund It" initiative, and the related report on which was released November 21, 2019. Commissioner Carr tied the FCC's actions to other government proceedings that identify security concerns about certain Chinese companies, including section 889 of the 2019 National Defense Authorization Act.

Commissioner Rosenworcel recently has been outspoken on national security, speaking November 20, 2019, at a Jackson, Mississippi meeting of the U.S. Chamber of Commerce, Competitive Carrier Association, and Department of Homeland Security's Rural Engagement Initiative.

In her view, the FCC has more work to do on network security. Commissioner Rosenworcel outlined several proposals:

1. She argues that software defined networks and open-radio access networks (O-RAN) should be researched and prioritized abroad and in standards bodies to help reduce dependencies on a few manufacturers, and have greater interoperability. She believes this can be advanced by the FCC in its new existing experimental 5G test beds in New York and Salt Lake City.
2. She argues that all IoT devices that emit radio frequencies should have to pass through an expanded FCC equipment authorization regime that incorporates security requirements, perhaps based on the emerging baseline at the National Institute of Standards and technology.
3. She urges "smarter spectrum policy" including mid-band auctions rather than high-frequency bands that are less efficient in rural areas. She says the next spectrum auction should include the 3.5 GHz band, first, and then the C-band.

Commissioner Starks urged the FCC to prevent untrustworthy equipment from entering our networks in the first place. He wants the FCC to be proactive on national security to avoid problems like untrustworthy equipment in the future. His recent report entitled *Security Vulnerabilities Within Our Communications Networks* calls for several actions and an expansive use of FCC authorities. Commissioner Starks also offered several proposals.

1. He calls for a National Security Task Force at the FCC, arguing that security reviews are inefficiently and unwisely divided across bureaus based on jurisdiction. He urges the FCC to issue a Public Notice about such a task force.
2. He says the FCC must promote growth of American innovation in 5G networks by exploring alternatives to traditional telecom networks, like cloud and software-based and O-RAN.
3. He urges the Commission to focus on security issues in undersea, submarine cables, which has been a frequent issue before the Committee on Foreign Investment in the United States.

Commissioner Starks is also reaching out to carriers on election security issues.

Conclusion

The FCC is poised to play an evolving role in national security issues, starting with this USF effort but perhaps taking on more. The FNPRM and future efforts will be important parts of the broader federal discussion about how to secure the nation's communications and internet infrastructure. Wiley Rein's Telecom, Media & Technology, National Security, Cybersecurity and Government Contracts practitioners can help navigate these shifting issues.