wiley

ALERT

Bill Requiring the "Rip and Replace" of Huawei and ZTE Equipment Heads to the President's Desk

March 2, 2020

Overview

On February 27, 2020, the Senate passed the Secure and Trusted Communications Networks Act of 2019 (H.R. 4998) (the Act or bill), which is now headed to President Trump for his signature. The bipartisan bill aims to counter national security threats in the communications supply chain by prohibiting the Federal Communications Commission (FCC or Commission) from subsidizing the acquisition or maintenance of telecommunications equipment or services from untrusted suppliers. It establishes a $1 billion reimbursement program for carriers with less than 2 million subscribers to "rip and replace" covered equipment. The Act also directs the FCC to maintain a list of suppliers that pose "unacceptable risk" to the national security of the United States and sets up a program for the federal government to share supply chain security risk information with trusted telecommunications providers and suppliers.

The Act, which was sponsored in the House by Energy and Commerce Committee Chairman Frank Pallone (D-NJ), Ranking Member Greg Walden (R-OR), Rep. Doris Matsui (D-CA), and Rep. Brett Guthrie (R-KY), and in the Senate by Senators Roger Wicker (R-MS), Tom Cotton (R-AR), Mark Warner (D-VA), Ed Markey (D-MA), and Dan Sullivan (R-AK), had passed the House of Representatives in mid-December 2019 on an unanimous voice vote. After a brief hold-up, the Senate passed the House version of the bill on February 27, 2020, in lieu of its own version that had passed the Senate Commerce Committee but never received a vote on the Senate floor, thus clearing the path for the

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

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Practice Areas

Telecom, Media & Technology

President's signature. Although the precise timing for signing the bill into law is not yet clear, it could align with the White House's planned 5G Summit for late March.

The Act builds upon the FCC's 2019 Supply Chain Order, which already prohibits the use of Universal Service Fund (USF) subsidies by carriers to purchase or obtain equipment or services produced or provided by a covered company, and designates Huawei Technologies Company (Huawei) and ZTE Corporation (ZTE) as covered companies for purposes of the prohibition. Under the Act, the Commission's 2019 Supply Chain Order stands, but only to the extent that such actions are consistent with the bill. The Commission is otherwise directed to adopt a new Report and Order implementing the statutory prohibition within six months from the bill's enactment.

Details of the Act

Generally, the Act prohibits the use of any Federal subsidies made available through the FCC (including USF funding) from being used to purchase, rent, lease, or otherwise obtain, as well as for the maintenance of, any "covered communications equipment or services," and establishes a reimbursement program for some communications carriers.

1. Establishment of a List of Covered Equipment and Services

Section 2 of the Act requires the Commission, within one year of enactment, to publish and maintain a list of "covered communications equipment or services" that could undermine the security of U.S. networks. Equipment or services must be placed on the list if produced or provided by an entity that "poses an unacceptable risk to the national security of the United States or the security and safety of United States persons" and is capable of:

- routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles;
- causing the network of a provider of advanced communications service to be disrupted remotely; or
- otherwise posing an unacceptable risk to the national security of the United States or the security and safety of U.S. persons.

In making these determinations, the FCC must rely on either:

- a specific determination made by any executive branch interagency body with appropriate national security expertise (including the Federal Acquisition Security Council);
- a specific determination made by the Department of Commerce under Executive Order 13873;
- inclusion in section 889(f)(3) of the 2019 National Defense Authorization Act (which includes telecommunications equipment produced by Huawei, ZTE, or any subsidiary or affiliate of such entities, among several others); or
- a specific determination by a national security agency.

The Act requires the FCC to periodically update and monitor the list for the inclusion or removal of communications equipment or services.

2. Prohibition of the Use Funds Administered by the FCC for Covered Equipment and Services

Section 3 of the Act prohibits the use of federal subsidies made available through programs administered by the FCC from being used to purchase, rent, lease, obtain, or to maintain any covered communications equipment or service previously obtained. This prohibition is effective 60 days after the Commission places such equipment or services on the covered list. The FCC must adopt, within 180 days of enactment, a Report and Order to implement such statutory prohibition, although it is not required to revisit prior efforts that are consistent with the Act.

While FCC rules adopted in the 2019 Supply Chain Order already prohibit universal service support for all equipment or services produced or provided by any company posing a national security threat, the legislation differs in that it more broadly prohibits any federal subsidy made available through a program administered by the FCC, not just through the universal service programs. At the same time, the prohibition is more narrowly applied to funds "to be used for the capital expenditures necessary for the provision of advanced communications service," which would seemingly exclude funds not used for the buildout of network infrastructure.

3. The Secure and Trusted Communications Networks Reimbursement Program

Section 4 of the Act requires the FCC to issue regulations, within one year of enactment, to establish a "Secure and Trusted Communications Networks Reimbursement Program" of $1 billion, to reimburse communications companies with 2 million or fewer customers for the costs associated with ripping and replacing covered equipment from networks. The reimbursement program must be separate from any Federal universal service program established under section 254 of the Communications Act of 1934, as amended (47 U.S.C. 254), but no money is actually authorized in the legislation to be appropriated by Congress.

Applicants for reimbursement under the program are required to provide initial reimbursement estimates at the time of application and to certify that they have developed a plan for the permanent removal, replacement, and disposal of covered equipment and services from their networks.

1. Trusted Equipment. As part of the program, the FCC is required to develop a list of suggested replacements of both physical and virtual communications equipment, application and management software, and services or categories of replacements. The list must be "technology neutral and may not advantage the use of reimbursement funds for capital expenditures over operational expenditures [.]"
2. Application Process and Restrictions on Reimbursement Recipients. The Act requires the FCC to approve or deny applications for reimbursement within 90 days of submission, although the agency may extend the deadline by up to 45 days if it needs additional time to review the applications. The FCC must afford reimbursement applicants 15 days to cure any material defects before denying an

application. If an application is granted, it prohibits a company from using reimbursement funds *or any other funds (including funds derived from private sources*) to purchase, rent, lease, or otherwise obtain covered communications equipment or service. Applicants must also consult and consider risk management practices including "the standards, guidelines, and best practices set forth in the cybersecurity framework developed by the National Institute of Standards and Technology."

3. Available funds. The FCC must make a reasonable effort to distribute funds under the program "equitably among all applicants for reimbursements." If the FCC determines that $1 billion is insufficient to fund all approved applications, the agency must contact the House and Senate Commerce and Appropriations Committees. However, the bill does not appropriate funds for this program.
4. Additional Reimbursement Program Details. Within one year of receiving reimbursement funds, recipients must have permanently removed, replaced, and disposed of any covered communications equipment or services. The FCC may grant a six-month extension if the supply of replacement equipment cannot meet the demand of reimbursement recipients. Individual extensions may be granted by the FCC upon petition by a recipient. Recipients must comply with FCC regulations governing the appropriate disposal of covered equipment and file status updates on the use of funds at least every 90 days. The FCC will make the status updates publicly available.

   To avoid waste, fraud, and abuse in the program, the Act directs the FCC to require recipients to submit spending reports and to perform regular audits and reviews of reimbursements, as well as random field investigations.

   The Act requires the FCC to commence a rulemaking proceeding, within 90 days of the enactment, to implement directives under the reimbursement program and to engage in an effort to educate eligible carriers on submitting applications. The FCC must complete the rulemaking within one year.

4. Reports to the FCC

Section 5 requires each provider of "advanced communications service" to submit an annual report to the FCC on whether the provider purchased, rented, leased, or otherwise obtained covered equipment and services in the preceding year. The term "advanced communications service" has the meaning given the term "advanced telecommunications capability" in section 706 of the Telecommunications Act of 1996 (47 U.S.C. 1302). In turn, the term "advanced telecommunications capability" is defined, "without regard to any transmission media or technology, as high-speed, switched, broadband telecommunications capability that enables users to originate and receive high-quality voice, data, graphics, and video telecommunications using any technology." If the provider certifies to the Commission that it does not have any covered communications equipment or services in their network, such a report is not required.

On February 26, 2020, and as part of its 2019 Supply Chain Order, the FCC announced an information collection to assess how much Huawei and ZTE equipment is in the networks of USF recipients and estimate how much it would cost to rip and replace such equipment. This mandate applies to Eligible

Telecommunications Carriers (ETCs) that are USF recipients, whereas the Act requires all providers of "advanced communications services" to submit an annual report to the FCC, or otherwise certify the nonexistence of covered equipment and services.

5. Connect America Fund Phase II Build-Out

Section 6 clarifies that if the prohibition on covered equipment and services prevents any Connect America Fund Phase II auction winners from meeting their build-out obligations, they may withdraw their application for Connect America Fund Phase II support without being found in default.

6. FCC Enforcement & Penalties

Section 7 gives the FCC authority to enforce the Act and any regulations promulgated under it, consistent with the Communications Act of 1934. A reimbursement program recipient found to have violated the Act or regulations:

- shall repay all reimbursement funds provided under the Program;
- shall be barred from further participation in the Program;
- shall be referred to all appropriate law enforcement agencies or officials for further action under applicable criminal and civil laws; and
- may be barred by the FCC from participation in other agency programs, including the federal USF programs.

7. Information Sharing Program

Section 8 of the Act requires the Administrator of the National Telecommunications and Information Administration (NTIA) within the Department of Commerce—in coordination with the Office of the Director National Intelligence, the Federal Bureau of Investigation, the Department of Homeland Security (DHS), and the FCC—to establish a program to share federal government information regarding supply chain security risks with trusted communications providers and trusted suppliers of communications equipment and services. The term "trusted" is defined, with respect to a provider of advanced communications service or a supplier of communications equipment or service, as an entity that the NTIA Administrator has determined is not "owned by, controlled by, or subject to the influence of a foreign adversary."

Activities under this program will include regular briefings and other events to share information with trusted providers of advanced communications service and trusted suppliers of communications equipment or services. Within six months from the enactment of the legislation, NTIA is directly to submit to Congress a plan to declassify relevant material, when feasible, and expedite and expand the provision of security clearances to facilitate information sharing of supply chain security risks. The head of NTIA must also ensure that the activities carried out through the program are consistent and integrated with, ongoing activities of the DHS and the Department of Commerce.

The Act requires the FCC to appoint to the Communications Security, Reliability, and Interoperability Council (CSRIC) and its working groups "at least one member to represent the interests of the public and consumers." Initial appointments must be made within 180 days of enactment.

For assistance from the Wiley team in understanding the potential impact of Act, please contact one of the authors listed on this alert.