

CLIENT ALERT

FCC Publishes Telecommunications Supply Chain Security Rule

Jan.21.2021

On January 13, 2021, the Federal Communications Commission (FCC) published [a final rule](#) that requires advanced communications providers to review their equipment and services within their networks and either: (1) certify that they do not include any covered equipment; or (2) file an annual report with the FCC that identifies covered communications equipment or services (as described below), details information about the equipment/service and their removal or replacement plan, and justifies the use of the equipment/service, among other things. Government contractors that have to make a representation under Section 889(a)(1)(B) of the FY2019 NDAA are challenged if they operate in rural locations where there may not be providers that do not use covered equipment or services. This rule may ultimately alleviate that issue for contractors by requiring and providing funding for removal and replacement of covered equipment and services. The new rule, which implements the Secure and Trusted Communications Networks Act of 2019, is effective March 15, 2021, with limited exceptions for the required reporting and parts of the rule's removal, replacement, disposal, and reimbursement requirements.

The rule establishes processes and procedures for the creation of a list of covered communications equipment and services determined to be a risk to national security ("Covered List"). The FCC's Public Safety and Homeland Security Bureau will include equipment and services on the Covered List, which is subject to modification, that (1) are produced or provided by any entity if the equipment or services pose an unacceptable risk to U.S. national security or U.S. persons, as specifically determined by certain agencies or departments; and (2) are capable of routing or redirecting user data traffic or permitting visibility into any user data or packets that the equipment or services transmit or handle, causing advanced communications service providers' networks to be disrupted remotely, or otherwise posing an unacceptable risk to U.S. national security or U.S. persons.

The rule also:

- Directs the FCC to develop a list of categories of suggested replacements for equipment and services included on the Covered List;
- Establishes the Secure and Trusted Communications Networks Reimbursement Program for those providers of advanced communications services with two million or fewer customers. Participants in the program must meet certain criteria and certify, among other things, that they have established a plan for the permanent removal and replacement of any covered communications equipment or services. The rule includes penalties for those reimbursement recipients who violate the Secure and Trusted Communications Networks Act of 2019. These penalties include reimbursing the government, barring from the reimbursement program, referral to criminal or civil law enforcement agencies, and barring from other FCC programs.
- FCC subsidies may not be used for the purchase or maintenance of covered equipment and services.
- Directs recipients of Universal Service Fund support to "rip and replace" covered equipment and services prior to receiving a funding commitment or support, unless they are participating in the reimbursement program.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Caroline E. Brown

Partner – Washington, D.C.
Phone: +1 202.624.2509
Email: cbrown@crowell.com

Adelicia R. Cliffe

Partner – Washington, D.C.
Phone: +1 202.624.2816
Email: acliffe@crowell.com

Kate M. Growley, CIPP/G, CIPP/US

Partner – Washington, D.C.
Phone: +1 202.624.2698
Email: kgrowley@crowell.com

Stephanie L. Crawford

Associate – Washington, D.C.
Phone: +1 202.624.2811
Email: scrawford@crowell.com