FCC Remains Focused on Communications Supply Chain Protection; Seeks Comment on Continued Implementation of Secure Networks Act

August 12, 2020

Protecting the U.S. communications supply chain from national security threats has become a priority for the Federal Communications Commission ("FCC" or "Commission") and the agency's recent Communications Supply Chain Protection proceeding resulted in new rules restricting the use of universal service support funds for certain equipment and services and the designation of Huawei and ZTE as national security threats to the communications networks and supply chain. The recently enacted Secure and Trusted Communications Networks Act of 2019 ("Secure Networks Act") requires the FCC to adopt additional communications supply chain protection measures and the Declaratory Ruling ("Declaratory Ruling") and Second Further Notice of Proposed Rulemaking ("Second FNPRM"), adopted by the FCC's at its July Open Meeting, continues the Commission's implementation of the Secure Networks Act. The Declaratory Ruling/Second FNPRM declares the Commission's compliance with the Secure Networks Act's federal funding prohibition requirement and seeks comment on the FCC's proposed interpretation and implementation of other provisions including key definitions and the identification of equipment and services subject to federal funding prohibitions.

Comments on the Second FNPRM are due by August 31, 2020 and reply comments are due by September 14, 2020.

FCC Declares Compliance with Secure Networks Act's Federal Funding Prohibition Mandate

Mirroring the Commission's November 2019 Supply Chain Protection Order in many respects, the Secure Networks Act, enacted in March 2020, seeks to protect the U.S. communications supply chain from equipment and services posing unacceptable national security risks. Among other mandates, Section 3 of the Secure Networks Act requires the Commission to adopt a Report and Order prohibiting federal funds, that are used for capital expenditures necessary to advanced communications services and made available in FCC-administered programs, from being used for certain services and equipment deemed to pose a national security threat. The Declaratory Ruling concluded that, although adopted prior to the Secure Networks Act, the Supply Chain Protection Order's prohibition on the use of federal universal service funds ("USF") for any equipment or service provided by a company posing a national security threat, was consistent with and "substantially implemented" the narrower prohibition, set forth in Section 3 of the Secure Networks Act.

Comments invited on FCC Proposed Interpretation and Implementation of the Secure Networks Act

Focusing on the Commission's proposed implementation of Sections 2, 3, 5, and 7 of the Secure Networks Act, the Second FNPRM invites comment on issues that could significantly affect telecommunications providers and advanced communications service providers that receive federal funds. Among other issues, the Commission seeks comment on the following:

Definitions of Key Terms - The Commission proposes to define two key terms - "advanced communications services" and "communications services and equipment" - used in the Secure Networks Act. Under the Commission's proposed definition, advanced communications services would use a "200 kbps in either direction" speed threshold to capture equipment that would not meet current advanced telecommunications capability speeds, such as the current 25 Mbps download/3 Mbps upload standard for fixed services, but nonetheless might pose a national security threat. In a proposal that the Commission describes as providing a bright-line rule for easy administration, "communications equipment and services" would be defined to include all of the services and equipment used in fixed and mobile broadband networks, provided they use or include electronic components.

Section 2 "Covered" Equipment and Services List – Section 2 of the Secure Networks Act requires the Commission to publish, for purposes of the federal funding usage prohibition, a list of "covered" communications equipment and services, that are deemed to present an unacceptable risk to national security (the "Covered List"). The Second FNPRM raises several questions regarding how to implement this mandate including, for example:

- Can executive branch agencies, such as Team Telecom or CFIUS, that are not specified in the Secure Networks Act, determine that equipment or service poses a national security risk (a "determination")?
- What is the required level of specificity for determinations, e.g., must a determination identify equipment model numbers or would the mere identification of an equipment or service provider qualify as a determination?
- What process should the Commission use to permit interested parties to clarify if a specific communications equipment or service is or is not on the Covered List?
- Because the Commission interprets the Secure Networks Act as requiring that the Covered List be published without a public comment period, the Second FNPRM comment cycle may be of particular interest to entities that could be subject to the Covered List prohibitions.

Section 3 Federal Funding Usage Prohibitions - Although the Commission declared its compliance with one of the Secure Networks Act's Section 3 mandates, the Second FNPRM tees up other Section 3 implementation issues for comment. Among other issues, the Commission seeks comment on adopting a new rule, prohibiting FCC-administered federal subsidies from being used to purchase or maintain items on the Covered List, to more closely align the Commission's current national security threat "designated entity" prohibition approach with the "designated equipment and services" approach of the Secure Networks Act. The Commission also recognizes that the Secure Network's Act's prohibition timing, requiring prohibitions be effective 60 days after a service or equipment is added to the Covered List, could affect existing contracts and requests comment on whether the Secure Networks Act permits the FCC to grandfather multiyear contracts or contracts with voluntary extensions.

Sections 5 and 7 Reporting and Enforcement – While they are important provisions, Sections 5 and 7 of the Secure Networks Act raise fewer implementation issues. Section 5 requires that advanced

communications providers submit annual reports regarding any “purchased, rented, leased, or otherwise obtained” covered equipment and services and include a “detailed justification” for obtaining the equipment and service. The Second FNPRM solicits comment on what must be included in the detailed justification, the proposed report contents, and the confidentiality of such reports. Section 7 directs the FCC to treat violations of the Secure Networks Act and related regulations in the same manner as violations of the Communications Act and also requires federal funding recovery for violations. Noting that the Commission has existing enforcement regulations, the Second FNPRM proposes to adopt regulations addressing only the Section 7 fund recovery requirement and seeks comment on any additional clarifications necessary to enforce the requirement.

Next Steps

The Commission’s Supply Chain Protection proceeding has been and remains active with industry participants initially weighing in on the Commission’s USF spending prohibitions and more recently commenting on the information collection addressing anticipated costs for removing and replacing equipment deemed to pose a national security threat. The Second FNPRM is likely to trigger similar levels of interest as industry participants assess the potential impact of the additional issues related to implementing the Secure Networks Act. Although the Commission has some time to implement those requirements – for example the covered equipment and services list has a required publication date of March 12, 2021 – based on the importance of the issue and the likely significant coordination and logistics necessary to implement the Secure Networks Act requirements, we anticipate that the proceeding, and further Commission action, will progress fairly quickly.

We will continue to monitor the Commission’s Supply Chain Protection efforts. Please reach out to us or your usual Kelley Drye attorneys if you have any questions.