wiley

ALERT

FCC Releases Proposal to Tackle Security in Equipment Authorizations, Spectrum Auction Certifications, and Beyond

June 22, 2021

On June 17, 2021, the Federal Communications Commission (FCC or Commission) voted unanimously to approve its Notice of Proposed Rulemaking (NPRM) and Notice of Inquiry (NOI) proposing significant changes to the FCC's equipment authorization regime and competitive bidding certification rules to further the goals of protecting the nation's communications networks and supply chains from equipment and services that pose an unacceptable risk to national security. This latest proposal builds upon the Commission's ongoing efforts to protect our nation's communications networks as well as other federal government efforts.[1] Comments on the NPRM and NOI will be due **30 days** after the item is published in the Federal Register and Reply Comments will be due **60 days** after publication.

At the Commission Meeting, Acting Chairwoman Rosenworcel explained how the FCC's proposal would spark progress on three lines of effort:

- Taking direct action to exclude untrustworthy equipment from the nation's communications networks.
- Speeding the way for trustworthy innovation and signaling that the United States is committed to developing a market for secure 5G equipment alternatives.
- Advancing a multifaceted, strategic approach to securing networks from all threats. She emphasized the need to secure the Internet of Things (IoT) by encouraging manufacturers to build security into products.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Amb. David A. Gross
Partner
202.719.7414
dgross@wiley.law

Thomas M. Johnson, Jr.
Partner
202.719.4550
tmjohnson@wiley.law

Meredith G. Singer
Partner
202.719.7507
msinger@wiley.law

Joshua S. Turner
Partner
202.719.4807
jturner@wiley.law

David E. Hilliard
Senior Counsel
202.719.7058
dhilliard@wiley.law

Practice Areas

Government Contracts
Internet of Things
National Security
Privacy, Cyber & Data Governance
Supply Chain and Transactional Support
Telecom, Media & Technology
Wireless

While the adopted item is mostly consistent with the circulated draft (see Wiley's Client Alert on the draft item), there are several noteworthy additions including:

- Questions for retailers on how they can help protect the integrity of the U.S. supply chain and voluntarily limit sales of equipment lacking appropriate security protections. Commissioner Starks noted that even with industry best practices, some equipment sold in the U.S. still lacks appropriate security protections, particularly "inexpensive equipment sold on large websites."
- A proposal that foreign applicants for equipment authorization have a registered U.S. agent for service of process. Commissioner Starks suggested this addition, noting prior enforcement actions against Chinese companies where the FCC had been unable to complete service of process or collect assessed forfeitures due to the lack of a U.S. agent.
- Questions regarding educating the public about the changes to the equipment authorization rules and the importance of security protections for their devices.
- An inquiry into the status of international supply chain standards and how to encourage greater participation in these efforts.
- The NOI now asks about emerging technologies to secure the IoT, such as RF fingerprinting. Commissioner Simington suggested this addition, noting that these technologies have matured since the last time the FCC considered them.

Wiley's team includes lawyers, engineers, and former policymakers that work at the cutting edge of federal supply chain oversight and national security. We work seamlessly across the Telecom, Media & Technology, National Security, Government Contracts, and Privacy, Cyber & Data Governance practices to help clients manage risk and shape new federal requirements. We have particularly deep experience with the FCC's equipment authorization regime and enforcement in this area, handled by former Office of Engineering and Technology's (OET) staff.

[1] *See, e.g.* FCC Imposes Security Prohibitions, Certifications, and Reporting Requirements for Providers of "Advanced Communications Services"; Biden's Cyber EO Aims to Improve Federal Security and Move Private Sector.