wiley

ALERT

# New FCC Proceeding to Tackle Security in Equipment, Auctions, and Beyond

May 28, 2021

On May 27, 2021, the Federal Communications Commission (FCC or Commission) released a draft Notice of Proposed Rulemaking (NPRM) and Notice of Inquiry (NOI) proposing significant changes to the FCC's equipment authorization regime and spectrum auction certifications, intended to protect U.S. communications networks from equipment and services that pose an unacceptable risk to national security.

This item follows years of work by the FCC and other agencies on aspects of telecommunications equipment security. This new proceeding, *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program; Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program*, picks up on calls by Acting Chairwoman Jessica Rosenworcel to examine national security in equipment authorization proceedings[1] and recent calls by Commissioner Brendan Carr to exclude certain companies from the FCC's approval of equipment for sale in the United States.[2]

The item is expected to be voted on at the June 17, 2021 FCC Open Meeting. There is a short window of time in which to advocate for changes to the draft item before the Commissioners vote, and thereafter, the process will invite public comment. If the item is approved, comments will be due 30 days after publication in the Federal Register and reply comments due 60 days after publication.

The FCC has been increasingly active on national security issues, on its own and at the direction of Congress. Our team has been engaged on these and related issues, using a multidisciplinary

## Authors


Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Amb. David A. Gross
Senior Counsel
202.719.7414
dgross@wiley.law

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

Hon. Nazak Nikakhtar
Partner
202.719.3380
nnikakhtar@wiley.law

Joshua S. Turner
Partner
202.719.4807
jturner@wiley.law

Kurt E. DeSoto
Of Counsel
202.719.7235
kdesoto@wiley.law

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


## Practice Areas

National Security
Strategic Competition & Supply Chain
Telecom, Media & Technology
Uncrewed Aircraft Systems (UAS)

approach to telecom and Information Communication Technology (ICT) security that draws on telecom, trade, government contracts, and export control experts. Our team includes former senior government officials that led United States policy at the U.S. Departments of Commerce and State, and at the Federal Communications Commission.

This item has three main parts, listed below.

**A Notice of Proposed Rulemaking to Change the Equipment Authorization Rules**

The FCC's equipment authorization regime is intended to ensure that devices that emit radiofrequency (RF) energy imported to or marketed within the United States comply with the Commission's technical requirements. The equipment authorization rules are designed to minimize the potential for harmful interference, and to ensure that devices comply with certain other Commission rules, such as human RF exposure limits, hearing aid compatibility requirements, and labeling obligations.

The FCC's rules currently specify two procedures for obtaining equipment approval: (1) certification and (2) Supplier's Declaration of Conformity (SDoC). Certification is the more rigorous approval process and it requires testing by an FCC-recognized accredited testing lab and filing a detailed application for approval with an FCC-approved Telecommunication Certification Body. The SDoC process, by comparison, does not require filing a detailed application for approval, but nevertheless still requires some device testing.

The existing equipment authorization rules do not include any specific provisions addressing device security or fitness for any particular purpose. In particular, the rules do not address the list of "covered communications equipment and services" (Covered List) that the Commission otherwise has determined pose security risks. The draft NPRM proposes to change this approach, and add security concerns into the equipment authorization process.

- The FCC proposes to prohibit all future authorizations for equipment on the Covered List, regardless of whether the equipment would be subject to the certification or Supplier's Declaration of Conformity process.
- The FCC proposes precluding "covered equipment" from being exempted from the equipment authorization process.
- The FCC proposes revoking existing equipment authorizations for covered equipment.

**A Notice of Proposed Rulemaking to Add Competitive Bidding Certifications**

As part of its competitive bidding procedures, the Commission has required spectrum auction applicants to make various certifications on their auction applications to qualify as a prospective bidder. The substance of the required certifications varies. For example, among other things, applicants must make certifications regarding joint bidding arrangements, whether they are in default on any Commission licenses or debts, and whether they have been barred by any agency of the Federal Government from bidding on a contract, participating in an auction, or receiving a grant. If an auction applicant is unable to make the required

certifications, its application to participate in the auction is dismissed.

- The FCC will propose to require an applicant to participate in competitive bidding to certify that its bids do not and will not rely on financial support from any entity that the Commission has designated as a national security threat to the integrity of communications networks or the communications supply chain.

**A Notice of Inquiry Raises Questions About the FCC's Role and the Future of Agency Activity**

The NOI delves into several open issues, but does not propose any specific rules at this time. NOIs are often used by the agency to gather information and identify positions on new areas of regulation or oversight. This is an important opportunity to help shape the future of Commission activity in emerging areas like Internet of Things (IoT) and cybersecurity.

- The NOI asks about how the Commission can leverage its equipment authorization program to help address the particular security risks that are associated with IoT devices.
- Should the Commission encourage manufacturers of IoT devices to follow the guidance in the National Institute of Standards and Technology's (NIST's) Internal Report 8259, Foundational Cybersecurity Activities for IoT Device Manufacturers, which was created in 2020 as flexible guidance for manufacturers of an array of IoT devices?
- If the FCC were to utilize the equipment authorization process to incentivize better cybersecurity practices, either for all devices or specifically for IoT devices, what form should such provisions take and how would such a program be structured most effectively?
- The FCC seeks comment on a Consumer Technology Association white paper, *Smart Policy to Secure Our Smart Future How to Promote a Secure Internet of Things for Consumers.* That paper encouraged public-private partnerships rather than rules or certification regimes to address cybersecurity.
- Should the FCC participate in the IoT cybersecurity labeling program mandated by President Biden's Executive Order (EO) on Improving the Nation's Cybersecurity? If so, how?
    - The Cybersecurity EO directs several different agencies to begin implementing ambitious steps to modernizing the nation's cyber defenses, including removing barriers to information sharing between government and the private sector, modernizing and implementing stronger cybersecurity standards in the federal government, improving software supply chain security, and improving detection and remediation of cyber incidents. The EO directs NIST and the Federal Trade Commission to identify cybersecurity criteria for a consumer labeling program. The FCC, as an independent agency, is not mentioned in the EO.

This new proceeding is a broad and important effort by the Commission to modify several regulatory regimes to address complex security issues. It builds on prior work by the Commission and other agencies to secure the ICT supply chain, including the FCC's proceeding banning the use of Universal Service Funds to purchase equipment on the Covered List and the Department of Commerce's proceeding on review of ICT transactions involving "foreign adversaries," and raises important issues of regulatory process, inter-agency collaboration, FCC jurisdiction, and more. It comes alongside a proposal by Senator Marco Rubio (R-FL) to narrowly adjust

the FCC's equipment authorization regime to exclude certain companies that the federal government has determined pose security risks.[3]

The FCC's activities here will have impacts on trade policy and other supply chain work across government from the Commerce ICT rule to the Federal Acquisition Supply Council. It could open the door to broader obligations on entities seeking equipment authorization or to participate in various FCC activities.

***

Our 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 OET staff.

---

1 *See, e.g.* Statement of Commissioner Jessica Rosenworcel, *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Program*, WC Docket No. 18-89, 34 FCC Rcd 11423, https://docs.fcc.gov/public/attachments/FCC-19-121A5.pdf (Nov. 26, 2019).

2 *See, e.g.* FCC, News Release, *Carr Urges Stronger Response to Communist China's Security Threats and Xinjiang Genocide*, https://docs.fcc.gov/public/attachments/DOC-371210A1.pdf (Mar. 30, 2021).

3 https://www.rubio.senate.gov/public/_cache/files/680f3b00-ffed-4c6c-8e59-05a83263a4ac/E4AC70E876A2DF146A4223CD7FF4C47F.oll21663.pdf