wiley

ALERT

Sweeping FCC Inquiry on Cyber and IoT

December 19, 2016

The Federal Communications Commission's (FCC or Commission) Public Safety and Homeland Security Bureau (PSHSB) issued a Notice of Inquiry (NOI) on *Fifth Generation Wireless Network and Device Security*, PS Docket No. 16-353, which the Commission had previewed in its July *Spectrum Frontiers Report and Order*. The NOI will have a 90-day comment period after Federal Register publication.

The PSHSB NOI poses over 130 questions about 5G security—from encryption and software upgrades to DDoS attacks and device security. It aims to "accelerate the dialogue around the critical importance of the early incorporation of cybersecurity protections in 5G networks, services, and devices." NOI ¶ 2. This inquiry comes amid ongoing activity at National Institute of Standards and Technologies, the U.S. Department of Homeland Security, and in the FCC's Communications Security, Reliability, and Interoperability Council and the Technical Advisory Council. ¶ 4.

Its questions include conceptual issues, like "[w]ho should be responsible for cyber protections for a device, or should responsibility be shared in some recognizable manner across the 5G ecosystem?" ¶ 5. And it poses detailed questions about technology and operation of wireless systems, devices and innovation, as well as threats and defenses. Though the 5G ecosystem is still nascent, the NOI seeks to build "a solid foundation of facts about 5G security in order to further identify potential issue areas and solutions." ¶ 7.

The NOI asks about authentication, encryption, physical security, device security, protecting 5G networks from cyber attacks (specifically DoS and DDoS), patch management, and risk segmentation of networks." *Id.* Each topic has many questions, some touching on issues already under consideration. For example, the NOI asks about software updates, which the FCC and Federal Trade

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Telecom, Media & Technology

Commission (FTC) are currently examining. *See* Letter from Jon Wilkins, Chief, Wireless Telecommunications Bureau, to Carriers (May 9, 2016).

Beyond these many issues, the PSHSB identifies additional wide ranging 5G security considerations, including:

- **Assignment of responsibility**. The PSHSB asks "[w]hat roles can service providers and device manufacturers play to reduce security risk for various communities of interest? How should service providers, device manufacturers, standards bodies, and the Commission coordinate their efforts?" ¶ 32.
- **Critical Infrastructure and Supply Chain**. The NOI asks about how the Internet of Things (IoT) affects critical infrastructure, and about supply chain issues. ¶ 34-35. The PSHSB asks again about responsibilities: "who should be responsible for assuring cyber security across the 5G ecosystem, what principles should guide the management of cyber risk, and how cyber risk should be managed within companies?" ¶ 37.
- **Information-sharing**. The PSHSB seeks input on "how the 5G ecosystem will share information about cyber threats and concerns" including whether the FCC should pursue an Information Sharing and Analysis Organization (ISAO) for 5G. ¶ 38
- **Costs and Benefits; DDoS Attacks**. It asks about the "public harm expected to result from failure to integrate confidentiality, integrity, and availability into 5G networks through authentication, encryption, physical and device security, protecting against DoS attacks, patch management, and risk segmentation. Could failure to implement these measures decrease broadband adoption and detract from its productive economic use?" ¶ 41.
- **Public Safety Impacts**. The PSHSB asks about "the security implications of linking or integrating 5G networks with IP-based public safety communications platforms." ¶ 44. It posts numerous questions about next-generation services for first responders.

****

As the FCC explores its role in cybersecurity, the PSHSB seeks input on numerous complex issues. This NOI comes in the waning days of current FCC leadership, but it may influence future FCC cyber activity.