Cooley

FCC Dives into Cybersecurity for Next Generation Wireless IoT Networks

December 21, 2016

The Federal Communication Commission's Bureau of Public Safety and Homeland Security has released a Notice of Inquiry ("NOI") seeking information on the best ways to secure the next generation of wireless technology, known as 5G. A key function of this new technology will be to connect Internet of Things ("IoT") devices. An NOI often is the first step in the development of regulations, although it is unclear whether a new, Republican-controlled FCC will view the agency as having sufficient jurisdiction to address cybersecurity. The NOI comes at the same time that a wide range of providers and trade associations have asked the FCC to rescind the cybersecurity reporting requirements adopted as part of its Spectrum Frontiers Order, which allocated millimeter wave (above 24 GHz) frequencies for 5G and other uses.

The notice describes the overarching security framework as one that ensures the confidentiality, integrity and availability (or CIA) of the network and connected devices. It focuses, particularly, on the well-established notion of security-by-design. Instead of security being an afterthought or "bolt-on" concept, the NOI focuses on a "comprehensive long-term strategic framework" for security, including such core concepts as authentication, encryption, physical network and device security, protection against DoS attacks, patch management and risk segmentation.

The notice also asks for comment on the roles and responsibilities of different participants in 5G (including users and device manufacturers), costs and benefits of security efforts and how to address security in public safety networks. Notably, the NOI observes that responsibility for cyber protection may need to be shared by all stakeholders (including end users) when securing the 5G infrastructure. Comments on the NOI will be due 90 days after notice of the NOI is published in the Federal Register and reply comments will be due 120 days after publication.

The Bureau recognizes that government agencies, such as NIST, are also addressing IoT security and that its efforts cannot occur in a vacuum. It seeks comment on ways to coordinate with, and build on, their efforts. For example, the NOI cites the NIST risk management cybersecurity framework on which other efforts are already being built. The Bureau also seeks comment on the use of Information Sharing and Analysis Organizations ("ISAOs") as a mechanism for private sector information sharing in the 5G ecosystem. In part because of the passage of the Cybersecurity Information Sharing Act of 2015, the notion of information sharing amongst similarly situated participants has become a critical tool in fighting cybercrime. One or more industry ISAOs could provide a useful mechanism for any number of IoT stakeholders.

Regardless of the ultimate outcome of this NOI, it presents an opportunity for participants in the IoT ecosystem, including equipment and software developers, to discuss how security is being built into next generation wireless networks and devices, or, alternatively, to outline their security concerns. The record developed in this proceeding may help inform the government generally as Congress and other agencies continue their oversight in this area.

The Communications and the Privacy & Data Protection Practice Groups at Cooley have highly complementary skills that uniquely situate the firm to help companies address IoT, FCC and related issues. The Communications Group has a deep and sophisticated understanding of communications networks and how they are regulated, while the Privacy & Data Protection Group has technical and substantial experience in assessing risks and responding to cybersecurity threats. Cooley has, for example, been instrumental in helping various industry sectors develop information sharing ecosystems and establish ISAOs. We can assist IoT participants in preparing useful and effective comments in this and related FCC proceedings.

Key Contacts

J.G. Harrington Washington, DC	jgharrington@cooley.com +1 202 776 2818
Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090