wiley

ALERT

FCC Wades into Cybersecurity - Regulation on the Horizon?

July 25, 2014

Today, the Federal Communications Commission's (FCC) Public Safety and Homeland Security Bureau released a Public Notice asking for input from "members of the Internet Community" and other stakeholders on industry's implementation of various cybersecurity recommendations previously developed by the FCC's third Communications Security, Reliability and Interoperability Council (CSRIC III), an advisory committee that makes recommendations to the FCC. Cybersecurity has been on the FCC's radar for some time, though with this Public Notice, the FCC may be to inching closer to a regulatory and oversight paradigm.

Communications industry effort on cyber is underway in companies, industry groups, and in the CSRIC working group, which in its current iteration—Working Group 4—is working to update best practices and bring them into alignment with the Cybersecurity Framework developed by the National Institute of Standards and Technology (NIST) earlier this year under President Obama's Executive Order, No. 13636 (Feb. 12, 2013). The communications industry worked with NIST on its Framework, and many in the private sector have urged the government to foster and evaluate use of the Framework before considering further steps.

Nonetheless, FCC Chairman Wheeler has made clear that he expects industry to take action, and that the agency is poised to step in to promote a "new regulatory paradigm." Chairman Tom Wheeler, Remarks at the American Enterprise Institute (June 12, 2014). Legislators have questioned the FCC's intentions and authority to impose obligations in this area, and recently "caution[ed]" the FCC to "resist the temptation of regulation" because of its "potential negative impact" on the private sector. Letter from Congressmen Rogers and

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Telecom, Media & Technology

Pompeo to FCC Chairman Tom Wheeler (June 16, 2014).

With this Public Notice, the FCC is signaling that it is serious about cyber and also perhaps that the risk of regulatory activity is real. It seeks comment on the "implementation and effectiveness of the CSRIC III recommendations and/or alternatives" that have been developed since they were produced. According to the FCC, CSRIC III in 2012 "unanimously adopted voluntary recommendations for Internet service providers (ISPs) to combat three major cybersecurity threats: (1) botnet attacks; (2) domain name fraud; and (3) Internet route hijacking," and CSRIC III also "recommended that the FCC encourage ISPs to implement source-address filtering to prevent attackers from spoofing IP addresses to launch DDoS attacks," by implementing certain best practices.

The Public Notice now asks for updates on progress and barriers to implementation of the recommendations, as well as for "success stories or breakthroughs." The FCC seeks to understand commenters' views and plans for "full implementation," and information about the recommendations' efficacy in mitigating cyber risk.

The communications industry has been addressing security in Congress, in CSRIC, at NIST, and the Federal Trade Commission. Now the FCC is publicly entertaining a more muscular role, beginning with an apparent attempt to demand some accountability. This raises important questions about the FCC's goals, as well as its continued adherence to longstanding federal policy to leave the Internet and mobile ecosystems free to manage and develop technical and operational solutions.

Comments on the Public Notice are due by September 26, 2014 and may be submitted under the FCC's rules for confidential treatment, as explained in the Public Notice.