Published on *The National Law Review* https://www.natlawreview.com

Telecom Alert: 911 Reliability Certification System Open; NTIA Seeks Middle Mile Reports Input; SEC, NIST Release New Cybersecurity Measures; Cybersecurity Labeling Program Pleading Cycle [Vol. XX, Issue 35]

Article By:

Jaimy "Sindy" Alarcon

Jim Baller

Timothy A. Doughty

Gregory E. Kunkle

Casey Lide

911 Reliability Certification System Open

Last week, the FCC's Public Safety and Homeland Security Bureau announced that the Commission's 911 Reliability Certification System is now open for filing annual reliability certifications. Under FCC rules, covered 911 services providers must take reasonable measures to provide reliable 911 service with respect to (i) 911 circuit diversity; (ii) central office backup power; and (iii) diverse network monitoring. Providers must certify as to their compliance with each of these requirements or to their implementation of reasonable alternative measures. Annual reliability certifications are due on October 16, 2023..

NTIA Seeks Middle Mile Reports Input

The National Telecommunications and Information Administration ("NTIA") issued a notice last week seeking input on modifying the reports that recipients of Middle Mile Broadband Infrastructure Program funding will be required to submit twice a year. Specifically, NTIA seeks comment on its proposal to add eleven questions regarding equipment purchases such as describing where the purchase will be located and how it will be used as well as the country from which the purchase is sourced. Comments are due by October 23, 2023.

SEC Finalizes Data Breach Reporting and Cybersecurity Disclosure Rules; NIST Releases Cybersecurity Framework 2.0

Two recent federal agency actions provide new cybersecurity rules and guidance and demonstrate how the landscape is changing. Earlier this month, the U.S. Securities and Exchange Commission ("SEC") adopted new rules that will (among other things) require publicly traded companies to disclose "material" cybersecurity incidents on SEC Form 8-K within four business days and make certain cybersecurity disclosures. In addition, the National institute of Standards and Technology released its latest Cybersecurity Framework, which now includes a section on corporate governance. Cybersecurity issues are directly related to environmental and social governance reporting issues and are increasingly important to businesses from a compliance and governance standpoint. The new SEC requirements have garnered industry criticism, and industry organizations are seeking a delay in the September 5, 2023, effective date. A more detailed article describing these agency actions is available at our website.

Cybersecurity Labeling Program Rules Pleading Cycle

As we previously reported, the FCC recently issued a Notice of Proposed Rulemaking seeking comment on rules creating a voluntary cybersecurity labeling program that would provide consumers with information about the security of Internet-enabled devices. The NPRM was published in the Federal Register last week. The FCC aims to improve consumer confidence and understanding of the security of connected devices by labeling smart devices and products that meet widely accepted security and privacy standards with the U.S. Cyber Trust Mark Logo. These standards would be based on criteria developed by NIST. Comments and reply comments are due by September 25 and October 10, respectively.

Thomas B. Magee, Tracy P. Marshall, Kathleen Slattery Thompson, Sean A. Stokes, and Wesley K. Wright also contributed to this article.

National Law Review, Volumess XIII, Number 241