Cooley

March 24, 2015

An industry-led committee advising the Federal Communications Commission ("FCC") on cybersecurity released its final report on best risk management practices tailored to each of five main industry segments—broadcasting, satellite, cable, wireless and wireline. The report's primary objective is to ensure that companies have taken sufficient steps to give the FCC and the public assurance that communications providers are managing cybersecurity risk. The committee report concludes that it is not a matter of if a communications company will be attacked, but when, rendering knowledge of potential threats "essential." The report adapts to the communications sector the cybersecurity risk management framework ("NIST Cybersecurity Framework") developed by the National Institute of Standards and Technology.

The report helps companies within each segment of the communications industry identify vulnerabilities and the most critical practices to incorporate when developing a company-wide risk management structure. The 400 page report provides specific guidance to small and medium-sized communications companies throughout all industry segments. The report also recommends a number of actions that the FCC should take to help ensure that communications companies implement the guidance provided in the report.

As an example of segment specific guidance, the report defines critical infrastructure for broadcasters as "maintaining on-air operations in order to deliver news, weather, critical public warning, and emergency information to the communities that they serve." The report also notes the increasing reliance on internet protocol-based infrastructure for core on-air operations. It developed four schematic models of different basic network architectures, ranging from small local TV and radio broadcast stations, to large national broadcast networks, to help companies identify the assets that require threat analysis. The report then maps to the four primary broadcast architectures each of the 98 risk management activities in the NIST Cybersecurity Framework. These risk management activities, tailored for the communications sector, correspond to the core functions specified in the NIST Cybersecurity Framework—specifically, Identify, Protect, Detect, Respond, and Recover. These core functions allow for common discussions about cybersecurity and risk management across a range of stakeholders. In performing this mapping, the CSRIC provides guidance on which activities are most critical to each of the different architectures.

The report contains recommendations to the agency to foster voluntary compliance and to continue to play an oversight role, including:

- Initiating voluntary, periodic confidential company-specific meetings to describe the company's efforts to adopt risk management practices, with the Department of Homeland Security ("DHS") in attendance;
- Encouraging and facilitating the sharing of information regarding cyber threats among communications companies;
- Promoting the voluntary use of the NIST Cybersecurity Framework and coordinate with states and other federal agencies to avoid duplicative efforts;
- Utilizing the extent of network availability as a meaningful indicator of successful cybersecurity risk management implementation;
- Encouraging the dissemination of the report to the management and staff responsible for cybersecurity inside communications companies; and
- Encouraging communications companies to share relevant threat intelligence information with other stakeholders, consistent with applicable law (*e.g.* laws that may impose liability).

The report also contains recommendations to companies in the communications sector that can be used to provide "macro-level" assurances that cybersecurity is a priority and to improve the overall cybersecurity health of those companies:

- Participation in DHS' Critical Infrastructure Cyber Community C3 Voluntary Program, which will increase awareness of cybersecurity risk management issues and the use of the NIST Cybersecurity Framework.
- Establishment of an effective governance structure that deals with cyber risk in a way that leads to a holistic assessment of the organization's risk posture.
- Sharing cybersecurity responsibilities among various communications stakeholders, coupled with interactions with other

sector stakeholders, can help make the communications infrastructure more secure.

The FCC is seeking public comment on the report's recommendations and overall utility. Comments are due May 29, 2015 and reply comments are due June 26, 2015. The agency also plans to initiate a pilot program to develop appropriate metrics to measure the efficacy of risk management practices.

There is clearly an expectation that companies within each of the industry segments will carefully review the guidance provided in the report and take reasonable steps to incorporate cybersecurity risk into the company's overall risk management governance structure. Although no rules are currently contemplated, the FCC Chairman has made clear that inadequate industry response to voluntary measures can lead to regulation.

The Communications Practice Group and the Privacy & Data Protection Practice Group at Cooley have highly complementary skills that uniquely situate the firm to help companies address the issues in the Report. The Communications Group has a deep and sophisticated understanding of communications networks while the Privacy & Data Protection Group have technical expertise and substantial experience in assessing cyber risks and responding to cybersecurity threats. We can help you understand the Report and how it applies to your organization. We can also assist in drafting comments for submission. Further, for organizations that are ready to implement the Framework, we bring to the table a well-seasoned team of communications and infosec legal professionals that can assist in implementing the Framework.

This content is provided for general informational purposes only, and your access or use of the content does not create an attorney-client relationship between you or your organization and Cooley LLP, Cooley (UK) LLP, or any other affiliated practice or entity (collectively referred to as "Cooley"). By accessing this content, you agree that the information provided does not constitute legal or other professional advice. This content is not a substitute for obtaining legal advice from a qualified attorney licensed in your jurisdiction, and you should not act or refrain from acting based on this content. This content may be changed without notice. It is not guaranteed to be complete, correct or up to date, and it may not reflect the most current legal developments. Prior results do not guarantee a similar outcome. Do not send any confidential information to Cooley, as we do not have any duty to keep any information you provide to us confidential. When advising companies, our attorney-client relationship is with the company, not with any individual. This content may have been generated with the assistance of artificial intelligence (AI) in accordance with our AI Principles, may be considered Attorney Advertising and is subject to our legal notices.

# Key Contacts



| | |
|---|---|
| Randy Sabett<br>Washington, DC | rsabett@cooley.com<br>+1 202 728 7090 |



This information is a general description of the law; it is not intended to provide specific legal advice nor is it intended to create an attorney-client relationship with Cooley LLP. Before taking any action on this information you should seek professional counsel.

Copyright © 2023 Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304; Cooley (UK) LLP, 22 Bishopsgate, London, UK EC2N 4BQ. Permission is granted to make and redistribute, without charge, copies of this entire document provided that such copies are complete and unaltered and identify Cooley LLP as the author. All other rights reserved.