SQUIRE PATTON BOGGS

FIRST-TIME EVER CYBERSECURITY MEASURES ADOPTED FOR COMMUNICATIONS SECTOR

On March 18, 2015, the Federal Communications Commission's (FCC) Communications Security, Reliability, and Interoperability Council (CSRIC) unanimously adopted a 415-page report with guidance and recommendations for voluntary cybersecurity protections for the communications sector in the United States: "Cybersecurity Risk Management and Best Practices Working Group 4: Final Report" (Final Report).

Background

President Obama's Cybersecurity Executive Order was issued in February 2013 (Cybersecurity Executive Order) and focused on 16 Critical Infrastructure sectors, one of which is the communications sector. Yet of all of the sectors, the communications sector is only one of two that is not regulated for cybersecurity at all – causing some friction with other sectors including energy and banking/financial services, which rely heavily on the communications sector and that have publicly expressed concerns about the sector.

In March of 2014, the FCC Chairman Wheeler advocated that the communications sector voluntarily take the lead to improve industry cybersecurity risk management practices – or potentially face a mandatory or regulatory approach down the road.

The Cybersecurity Executive Order directed the creation of a voluntary public-private partnership working with the National Institute of Standards and Technology (NIST) of the US Department of Commerce. In February 2014, NIST released the "Framework for Improving Critical Infrastructure Cybersecurity" (NIST Cybersecurity Framework), and while the communications sector participated in the process, adoption was limited within the sector. As a result, in 2013 the FCC created a multidisciplinary group (Working Group 4) under the CSRIC to look at systemic cybersecurity risks against the sector and included a variety of other agencies, such as the US Department of Homeland Security (DHS), as well as other sectors, including the banking/financial services sector, in the working group.

Cybersecurity Risk Management and Best Practices Working Group 4: Final Report

Working Group 4 was charged with developing voluntary mechanisms for the communications sector that would give the FCC and the public assurance that the sector is taking the necessary steps to manage cybersecurity risk across their entire organization and businesses. These "macro-level" assurances can be tailored by individual companies to suit their unique needs, characteristics and risk exposure and tolerance. They should also be based on meaningful measures of successful and unsuccessful efforts to combat cybersecurity (outcome-based indicators rather than process requirements). Such assurances should enable "meaningful" assessments within an organization as well as externally, such as with business partners and vendors.

Working Group 4 was also directed to show how the communications sector can reduce cybersecurity risk by leveraging the NIST Cybersecurity Framework. In addition, the working group was asked to come up with implementation guidance for sector participants based on and adapting the NIST Cybersecurity Framework.

To inform the development of the voluntary mechanisms and implementation guidance, Working Group 4 examined five segment subgroups based on communications operating environments: broadcast, cable, satellite, wireless and wireline. Moreover, several "feeder" topics for each segment were identified and examined: cyber ecosystem and dependencies, top threats and vectors, framework requirements and barriers, small and medium businesses, and measurements.

Voluntary Mechanisms

The Final Report recommends three new "voluntary mechanisms" that build on the communications sectors' existing cybersecurity management structure and experience to provide the FCC requested "appropriate macro-level assurances" for the communications sector:

- Sector participation in FCC-initiated confidential company-specific meetings or other similar communication formats to share risk management practices as well as organizations' efforts to respond and recover from cyberattacks.
- Sector preparation of a Communications Sector Annual Report (SAR) to describe efforts to manage cybersecurity risks.
- Active sector participation in the Department of Homeland Security's (DHS) Critical Infrastructure Cyber Community C3 Voluntary Program.

The purpose of these voluntary mechanisms is to enhance the communications sector's cybersecurity risk management capabilities and promote the use of NIST Cybersecurity Framework throughout the sector. (Notably, companies' sharing of risk management information and practices under the first bullet would be covered by legal protections available from the DHS' Protected Critical Infrastructure Information program.)

Implementation Guidance

The Final Report notes that many communications companies already have "long-standing and mature" cybersecurity risk management capabilities that use widely recognized standards and guidelines. Nonetheless, the Final Report provides several "immediate and practical" recommendations for the communications sector. Consistent with the NIST Cybersecurity Framework's approach to taking a holistic approach to cybersecurity, the Final Report recommends that communications companies implement a dedicated, organization-wide cybersecurity risk governance process. In short, each company is advised to include cybersecurity as part of its overall risk management efforts. The Final Report, however, notes that how each company implements a cybersecurity risk management program will vary based on identified potential risks, risk tolerance and other factors.

The Final Report also includes appendices for each of the five segments that identify infrastructure core assets and services for each sector (broadcast, cable, satellite, wireless and wireline) and present use cases to suggest how cybersecurity risk management protocols and practices can be implemented for each segment.

The FCC is seeking public comments on the Final Report (PS Docket No. 15-68): Comments on May 29, 2015 and Reply Comments on June 26, 2015. The full 415-page report can be accessed online.

Contacts

Norma M. Krayem
Global Co-Chair, Data Privacy & Cybersecurity
+1 202 457 5206
norma.krayem@squirepb.com

Ann J. LaFrance
Global Co-Chair, Data Privacy & Cybersecurity
+44 207 655 1752
ann.lafrance@squirepb.com

Paul C. Besozzi
+1 202 457 5292
paul.besozzi@squirepb.com

Mark D. Johnson
+1 202 626 6265
mark.johnson@squirepb.com