KING & SPALDING

Client Alert

Data, Privacy & Security Practice Group

March 23, 2015

FCC Communications Security, Reliability, and Interoperability Council Working Group Issues Final Report on Cybersecurity Best Practices

A Federal Communications Commission (FCC) working group, Cybersecurity Risk Management and Best Practices Working Group 4 (WG4), of the Communications, Security, Reliability, and Interoperability Council (CSRIC) advisory committee issued its Final Report on March 18, 2015.[1]

The FCC renewed the charter of the CSRIC for the fourth time on March 19, 2013 for a period of two years.[2] One of the duties of the CSRIC from this Charter was to "[d]evelop and recommend best practices and actions the FCC can take to improve the security of mobile devices and networks."[3] As part of discharging those duties, the CSRIC established working groups including WG4.[4] CSRIC WG4 set out to "develop voluntary mechanisms to provide macro-level assurance to the FCC and the public that communications providers are taking the necessary corporate and operational measures to manage cybersecurity risks across the enterprise."[5]

WG4 delivered its Final Report for proposed adoption by the FCC on March 18, 2015.[6] The recommendations of the WG4 Final Report promote the voluntary use of the NIST Framework, a framework for improving critical infrastructure released by NIST in February 2014, among all the communication sector members.[7] The WG4 Final Report also sets out guidance to individual companies in implementing the NIST Framework, as well as additional sector-specific implementation resources.[8]

The WG4 Final Report sets forth three specific voluntary mechanisms to provide macro-level assurances that communications providers are appropriately managing cybersecurity risks.[9] The three voluntary mechanisms are:

1. FCC initiated confidential company-specific meetings.

2. Enhanced Sector Annual Report focusing on segment-specific cybersecurity risk management.

3. Active participation in DHS C^3 Outreach and Education.[10]

For more information, contact:

Phyllis B. Sumner
+1 404 572 4799
psumner@kslaw.com

Steven T. Snyder
+1 704 503 2630
ssnyder@kslaw.com

King & Spalding
Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600
Fax: +1 404 572 5100

www.kslaw.com

Each of these voluntary mechanisms incorporates interaction with the DHS, the communications sector's Sector Specific Agency (SSA).[11]

The WG4 Final Report recommends the establishment of a dedicated cross-enterprise cybersecurity risk governance function as a key objective for companies. It contains segment-specific guidance provided to broadcast, cable, satellite, wireless, and wireline companies through industry subgroups along with cyber risk management recommendations that apply to the sector across-the-board.[12] Companies are urged to review the WG4 report and the NIST Framework and distribute copies of those documents to company officers and personnel whose duties encompass cybersecurity management.[13] Companies are also urged to ensure that operators and vendors conduct their operations with cybersecurity diligence. Sharing of threat information throughout the sector is also encouraged.[14]

A comprehensive identification of sector-specific operation and technical resources to implement 98 subcategories of the NIST Framework is set forth in the WG4 Final Report.[15] Segment reports include information such as identification of in-scope NIST Framework subcategories for certain segments including prioritization information.[16] For example, the cable segment section contains 27 pages of information directed to address alignment of existing cybersecurity practices with the NIST Framework.[17] An architectural model describing cable networks, services, and assets is presented first.[18] The next part of the cable segment section identifies subcategories of the NIST Framework that are in-scope and provides a prioritization of each from Not Critical to Most Critical.[19] The cable segment section also outlines a hypothetical profile of how to use 24 priority practices and augments them with expected outcomes—for example, a priority practice is inventorying physical devices and the anticipated outcome is a complete inventory of physical devices and systems in direct support of critical (core) infrastructure. [20] The subgroups for the other segments (broadcast, satellite, wireless, and wireline) each took their own approach but offered similarly detailed guidance that can be used by sector organizations to manage cyber risk.

The WG4 Final Report provides organizations in the sector with guidance to take the necessary steps to manage cybersecurity and thereby reduce risk. Should it be adopted by the FCC, the guidance would be voluntary but represents the work of a large number of sector participants in analyzing the NIST Framework and providing comprehensive sector-specific implementation recommendations. In addition, the WG4 Final Report sets forth mechanisms to facilitate the exchange of knowledge to aid in managing cyber risk.

On March 19, 2015, the FCC issued a Public Notice seeking Comment on three aspects of WG4 Final Report.[21] Specifically, the FCC is seeking comments by May 29, 2015 on three issues:

> (1) In what ways the recommendations are sufficient to meet the FCC's goal of reducing cybersecurity risk and in what ways they might be improved, augmented or made more specific.
>
> (2) Comments on each of the three specific Voluntary Mechanisms enumerated above.
>
> (3) What barriers, if any, would inhibit industry's effective application of the voluntary mechanisms throughout the WG4 Final Report? What differences exist based on factors such as size? How might these barriers be mitigated.

Sector companies should consider submitting comments pursuant to this notice.

King & Spalding's Data, Privacy and Security Practice

King & Spalding is particularly well equipped to assist clients in the area of privacy and information security law. Our Data, Privacy & Security Practice regularly advises clients regarding the myriad statutory and regulatory requirements that businesses face when handling personal customer information and other sensitive information in the U.S. and globally. This often involves assisting clients in developing comprehensive privacy and data security programs, responding to data security breaches, complying with breach notification laws, avoiding potential litigation arising out of internal and external data security breaches, defending litigation, whether class actions brought by those affected by data breaches, third party suits, or government actions, and handling both state and federal government investigations and enforcement actions.

With more than 50 Data, Privacy & Security lawyers in offices across the United States, Europe and the Middle East, King & Spalding is able to provide substantive expertise and collaborative support to clients across a wide spectrum of industries and jurisdictions facing privacy-based legal concerns. We apply a multidisciplinary approach to such issues, bringing together attorneys with backgrounds in corporate governance and transactions, healthcare, intellectual property rights, complex civil litigation, e-discovery, government investigations, government advocacy, insurance recovery, and public policy.

---

[1] CYBERSECURITY RISK MANAGEMENT AND BEST PRACTICES WORKING GROUP 4: FINAL REPORT, (Mar. 2015) [hereinafter WG4 Final Report] *available at* http://transition.fcc.gov/pshs/advisory/csric4/CSRIC_WG4_Report_Final_March_18_2015.pdf.
[2] CHARTER OF THE FCC'S COMMUNICATIONS SECURITY, RELIABILITY, AND INTEROPERABILITY COUNCIL, (Mar. 19, 2013) [hereinafter Charter] *available at* http://transition.fcc.gov/bureaus/pshs/advisory/csric4/CSRIC%20Charter%20Renewal%202013.pdf .
[3] Charter at 1.
[4] *See* CSRIC IV WORKING GROUP DESCRIPTIONS AND LEADERSHIP (Update Oct. 23, 2014) [hereinafter WG Descriptions] *available at* http://transition.fcc.gov/bureaus/pshs/advisory/csric4/CSRIC%20IV%20Working%20Group%20Descriptions%2010%2023%2014.pdf .
[5] WG Descriptions at 5.
[6] WG4 Final Report.
[7] WG4 Final Report at 31; *see also* NATIONAL INSTITUTE FOR STANDARDS AND TECHNOLOGY, FRAMEWORK FOR IMPROVING CYBERSECURITY, 79 FR 9167 (Feb. 18, 2014) [hereinafter NIST Framework], *available at* http://www.nist.gov/cyberframework/upload/cybersecurity- framework-021214.pdf.
[8] *See* WG4 Final Report at 8-10.
[9] *See* WG4 Final Report at 6.
[10] WG4 Final Report at 7.
[11] *See* WG4 Final Report at 7.
[12] *See* WG4 Final Report at 5-6.
[13] WG4 Final Report at 10.
[14] WG4 Final Report at 10.
[15] WG4 Final Report at 12.
[16] *See, e.g.*, WG4 Final Report at 65-67 (*discussing* cable segment).
[17] WG4 Final Report at 63-90.

[18] WG4 Final Report at 68-73.
[19] WG4 Final Report at 74-86.
[20] WG4 Final Report at 88.
[21] FCC'S PUBLIC SAFETY AND HOMELAND SECURITY BUREAU REQUESTS COMMENT ON CSRIC IV CYBERSECURITY RISK MANAGEMENT AND ASSURANCE RECOMMENDATIONS *available at* http://www.fcc.gov/document/csric-iv-cybersecurity-risk-management-and-assurance-recommendations.