

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
CSRIC IV Cybersecurity Risk)	PS Docket No. 15-68
Management and Assurance)	
Recommendations)	

Comments of CTIA – The Wireless Association®

Thomas Power
Senior Vice President, General Counsel

Thomas Sawanobori
Senior Vice President, Chief Technology Officer

CTIA – THE WIRELESS ASSOCIATION®
1400 16th Street, NW, Suite 600
Washington, DC 20036
(202) 785-0081

May 29, 2015

TABLE OF CONTENTS

I.	INTRODUCTION AND SUMMARY	1
II.	THE CSRIC IV RECOMMENDATIONS UNQUESTIONABLY ADVANCE THE COMMISSION’S CYBERSECURITY GOALS	4
III.	APPLICATION OF THE VOLUNTARY MECHANISMS SHOULD ADHERE TO CERTAIN GROUND RULES TO PROTECT PARTIES AND ENSURE PRODUCTIVE INFORMATION SHARING	6
	A. Commission-convened confidential meetings	6
	B. Addendum to Communications Sector Annual Report	9
	C. Active participation in DHS C ³ program	11
IV.	THE COMMISSION SHOULD FOCUS ON PROVIDING PRACTICAL ADVICE FOR OVERCOMING BARRIERS TO THE EFFECTIVE APPLICATION OF THE CSRIC IV RECOMMENDATIONS.....	11
V.	CONCLUSION.....	13

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
CSRIC IV Cybersecurity Risk)	PS Docket No. 15-68
Management and Assurance)	
Recommendations)	

Comments of CTIA–The Wireless Association®

CTIA – The Wireless Association® (“CTIA”)¹ welcomes the opportunity to provide the following comments in response to the Public Notice in the above-captioned proceeding, by which the Public Safety and Homeland Security Bureau (“Bureau”) seeks feedback regarding the report on Cybersecurity Risk Management and Best Practices submitted by the fourth Communications Security, Reliability and Interoperability Council (“CSRIC IV”).²

I. INTRODUCTION AND SUMMARY

CTIA represents all contributors to the global wireless ecosystem, from manufacturers and carriers to software and application developers. Through collaboration and innovation, these contributors have led a mobile revolution that has transformed the global economy. CTIA is committed to protecting cybersecurity in today’s dynamic threat environment. Indeed, CTIA has worked for years with its members and policy makers on security and technology issues. The wireless industry has tremendous experience ensuring the reliability of communications, and it

¹ CTIA – The Wireless Association® is the international organization of the wireless communications industry for both wireless carriers and manufacturers. Membership in the organization covers Commercial Mobile Radio Service (“CMRS”) providers and manufacturers, including cellular, Advanced Wireless Service, 700 MHz, broadband PCS, and ESMR, as well as providers and manufacturers of wireless data services and products.

² See Public Notice, *FCC’s Public Safety and Homeland Security Bureau Requests Comment on CSRIC IV Cybersecurity Risk Management and Assurance Recommendations*, DA 15-354, PS Docket No. 15-68 (rel. Mar. 19, 2015) (“Public Notice”).

has great incentive to do so. As a result, it has long been a leader on cybersecurity, and is actively engaged through public-private partnerships in the U.S. and through international standards-setting bodies. As CTIA has described in other filings, these efforts have been highly effective in preventing, detecting, addressing, and mitigating cybersecurity threats.³

CTIA appreciates the continued focus that the Commission and the Bureau bring to cybersecurity in the communications sector, and commends them for their engagement with the private sector to address these challenges. CTIA thus is pleased to provide feedback on CSRIC IV's Cybersecurity Risk Management and Best Practices report ("CSRIC IV Report" or "Report").⁴

As discussed below, CTIA strongly supports the Report's recommendations. CTIA and its members were key participants in the preparation of the Report and in the development of the voluntary National Institute of Standards and Technology ("NIST") cybersecurity framework (the "Framework") that the Report implements. The Report is the most comprehensive Framework implementation proposal for any industry to date. It will ensure that the telecommunications industry takes the necessary corporate and operational measures to manage cybersecurity risk across each company. The Report goes beyond merely offering guidance for reducing cybersecurity risk to critical infrastructure, enterprises, and consumers; it provides detailed, scalable recommendations designed to apply to each segment of the communications industry. CSRIC IV's efforts have validated *both* the Cybersecurity Executive Order's mandate

³ See generally, e.g., Comments of CTIA – The Wireless Association®, Cybersecurity Working Group, DA 14-1066, at 5-10 (filed Sept. 26, 2014).

⁴ Communications Security, Reliability and Interoperability Council IV, *Cybersecurity Risk Management and Best Practices, Working Group 4: Final Report*, Mar. 2015, available at http://transition.fcc.gov/pshs/advisory/csric4/CSRIC_WG4_Report_Final_March_18_2015.pdf.

to develop an industry-led, voluntary, risk- and outcome-based framework over a prescriptive and inflexible one-size-fits-all compliance regime,⁵ and Chairman Wheeler’s call for a “new regulatory paradigm” characterized by a business-driven cybersecurity risk management approach.⁶ Indeed, this is precisely what the CSRIC IV Report has achieved.

CTIA urges the Commission to continue to support such voluntary, collaborative, industry-led efforts and to avoid regulation in this space. As discussed below, the Report envisions a role for the Commission in connection with the voluntary mechanisms for providing macro-level assurances.⁷ To the extent the Commission or the Bureau is inclined to assume a greater role in implementing these recommendations, it should take the following steps:

- Leverage the work of CSRIC IV by encouraging other industry sectors to develop similar detailed, scalable Framework implementation plans for companies in their industries;
- Foster communication and cooperation with the Commission’s international counterparts to ensure global implementation;
- Encourage broader involvement in this process beyond critical infrastructure by advocating for the NTIA proposal to convene non-critical infrastructure entities to address these issues;
- Help to ensure that voluntary cybersecurity mechanisms are effective by acknowledging and emphasizing that any information sharing is for non-regulatory purposes and subject to nondisclosure protections, consistent with the Protected Critical Infrastructure Information program administered by the Department of Homeland Security;
- Encourage the use of meaningful, forward-looking indicators to project cybersecurity trends; and

⁵ Executive Order 13636, *Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2013), <http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf>.

⁶ Remarks of FCC Chairman Tom Wheeler, American Enterprise Institute, Washington, D.C., June 12, 2014, at 1; *see also* Report at 4 n.7 (quoting the same statement).

⁷ *See infra* Section III.

- Participate in outreach and education efforts to help smaller and medium-sized companies overcome the various barriers to implementing those solutions.

II. THE CSRIC IV RECOMMENDATIONS UNQUESTIONABLY ADVANCE THE COMMISSION'S CYBERSECURITY GOALS

The Public Notice first asks whether the CSRIC IV Report's recommendations are "sufficient" to meet the Commission's goal of reducing cybersecurity risk to critical infrastructure, enterprises, and consumers, and whether any of those recommendations should be augmented or otherwise improved.⁸

The CSRIC IV Report clearly addresses and advances the Commission's stated objectives, in a number of ways. The Report provides industry with a risk-based and outcome-based approach for addressing cybersecurity threats, as opposed to a prescriptive checklist of processes and activities.⁹ As a result, the Report's approach is uniquely suited to the current environment, in which the threats are dynamic and persistent. It will enable industry not only to reduce risk by identifying and responding to threats, but also to anticipate them and take preventive measures. In addition, the Report provides a comprehensive alignment of the Framework with all five segments of the telecommunications industry, including wireless, allowing a flexible, segment-by-segment application of the Framework.

Moreover, as noted above, the Report provides the very sort of flexible paradigm that Chairman Wheeler envisions, permitting entities to modify their approach to respond to different risks and threats across different industry sectors as they evolve. By implementing the Report's recommendations, industry will ensure that networks are available to deliver critical services.

⁸ Public Notice at 2.

⁹ See, e.g., Report at 4 (stating that the voluntary mechanisms recommended in the Report "validate the advantages of a non-regulatory approach over a prescriptive and static compliance regime").

This outcome-based measurement will give companies the ability to assure the public, their shareholders, and their boards that their cybersecurity risk management policies and procedures protect the security of the Nation's networks. And finally, the Report's recommendations can scale from small and medium enterprises to large companies, allowing entities to adapt their particular cybersecurity efforts to fit their unique business models, infrastructure, and the assets they need to protect.

Because the CSRIC IV Report's recommendations are so comprehensive and complete, there should be no need for the Commission to augment or modify them in any way. Instead, CTIA and its members recommend that the Commission build on the work of CSRIC IV and the Report by using its demonstrated abilities as a convener to foster communication, awareness, and cooperation in the following ways.

First, the Commission should communicate and work with its counterparts for other industry sectors to leverage the work of CSRIC IV. By amplifying the work of CSRIC IV, the Commission can encourage other sector-specific agencies to facilitate industries' alignment of the Framework with various business models within industry sectors and can play a national leadership role in ensuring that all industry sectors are engaged in cybersecurity preparedness.

Second, the Commission is uniquely suited to promote international coordination and engagement. Because the Internet has no borders, cybersecurity is truly a global concern, and threats may come from anywhere. A number of national and global standard-setting groups play an important role in the global mobile ecosystem. The Commission is in a unique position to reach out to these groups and other players on a global level. It should liaise with its counterparts in other countries to ensure ongoing communication and coordination and to facilitate the development of global solutions to cybersecurity challenges.

Third, as the Commission no doubt is aware, the National Telecommunications and Information Administration (“NTIA”) at the Department of Commerce concurrently is seeking comment on its proposal to lead a multistakeholder process through its Internet Policy Task Force to develop a cybersecurity approach for all relevant industry sectors beyond critical infrastructure.¹⁰ The Commission should actively advocate for and endorse that proposal. The Commission has been an essential leader in the process thus far, and it should leverage the progress it has facilitated by working with others in government to close gaps with other sectors that fall outside the Commission’s jurisdiction.

III. APPLICATION OF THE VOLUNTARY MECHANISMS SHOULD ADHERE TO CERTAIN GROUND RULES TO PROTECT PARTIES AND ENSURE PRODUCTIVE INFORMATION SHARING

The Public Notice next seeks comment on three separate voluntary mechanisms that CSRIC IV recommended to ensure industry accountability.¹¹ The CSRIC IV Report thoroughly describes these proposed processes and the basic ground rules that should apply to them.¹² Rather than recount that discussion in full, CTIA members use this opportunity to emphasize several key points about each proposed mechanism.

A. Commission-convened confidential meetings

The first proposed mechanism involves confidential, company-specific meetings that the Commission would initiate.¹³ The Report makes clear that such meetings would be entirely

¹⁰ Department of Commerce, National Telecommunications and Information Administration, Request for Public Comment, *Stakeholder Engagement on Cybersecurity in the Digital Ecosystem*, 80 Fed. Reg. 14360 (Mar. 19, 2015).

¹¹ Public Notice at 2.

¹² *See, e.g.*, Report at 6-8, 25, 27-28.

¹³ Report at 7.

voluntary on the part of industry.¹⁴ The Commission’s core challenge, then, is to ensure that companies are properly incentivized to participate in the process and to facilitate a productive dialogue and exchange of information. To do that, the Commission should establish unequivocally, at the outset and throughout the process, that it will afford industry participants necessary protections.

Most important, the Commission should emphasize that it will conduct these meetings in conjunction with the Department of Homeland Security (“DHS”) and under the Protected Critical Infrastructure Information (“PCII”) program (the “PCII Program”), which DHS administers. The Report makes clear that the PCII Program is an integral (and explicit) component of the voluntary meetings,¹⁵ and for good reason: The PCII Program guarantees that certain information that industry discloses to the government in connection with cybersecurity risk management will not be publicly disclosed (under the Freedom of Information Act or similar State, local, tribal, or territorial disclosure laws) and will not be used in civil litigation or for regulatory purposes.¹⁶ Thus, the Commission can best ensure participation in, and the success of, these voluntary meetings by making clear that they will be conducted under the PCII Program. Indeed, Congress authorized DHS to establish the PCII Program over a decade ago

¹⁴ See, e.g., Report at 7 (stating that meetings would include those “individual companies that agree to participate”).

¹⁵ See, e.g., Report at 6-7 (specifically stating that companies electing to participate in these meetings would be afforded the protections that the federal government provides under the PCII program).

¹⁶ See Procedures for Handling Critical Infrastructure Information; Final Rule, 6 C.F.R. § 29.3 (2006).

precisely to incentivize private industry to share this kind of information with the government for this purpose.¹⁷

Although the Report suggests that a “legally sustainable” equivalent to the PCII Program could also suffice,¹⁸ it does not identify any such program or explain how the Commission could devise one itself. In fact, attempting to administer a duplicate protection process for information sharing is both unnecessary (given that a time-tested and widely used one is available) and counter-productive (given that an alternative to the PCII program would take far more time to develop and implement, and even more time to gain a requisite level of trust from industry). Accordingly, the Commission should embrace the Report’s recommendation to rely on the PCII Program and work to eliminate any ambiguity or confusion about its applicability.

Further, given DHS’s role in administering the PCII Program, DHS participation in the Commission-initiated meetings is essential. The Report itself contemplates coordination between the Commission and DHS and specifically proposes that the periodic meetings be attended by “the FCC, DHS, and individual companies.”¹⁹ DHS attendance at these Commission-initiated meetings thus would be fully consistent with the Report’s recommendations, in addition to being highly practical in light of its important role in administering the PCII Program.

Consistent with the PCII Program’s restrictions, the Commission should make clear that it will conduct these voluntary meetings solely for non-regulatory purposes, and it will not use any information that companies reveal during these meetings for any rulemaking, litigation, or

¹⁷ See Homeland Security Act of 2002, 6 U.S.C. §§ 131 *et seq.*

¹⁸ See, e.g., Report at 7.

¹⁹ Report at 7; see also, e.g., *id.* at 358, 368 (recommending “annual meetings between the [Commission], DHS, and individual companies”).

other such purposes. Equally important, the information that industry reveals in these meetings must be protected from FOIA requests and other disclosures. The Commission should make these limitations explicit and emphasize them throughout the process. Doing so will incentivize companies to participate.

Finally, CTIA expects that the Commission-initiated meetings will be more useful for smaller companies that generally lack the resources to understand and address cybersecurity challenges. The Commission thus should focus on engaging these entities, as opposed to larger companies, which have more resources and a high level of sophistication with respect to cybersecurity matters.

B. Addendum to Communications Sector Annual Report

The Report also recommends including a new component in the Communications Sector Annual Report (“CSAR”) that would provide indicators of successful segment-specific cybersecurity risk management.²⁰ This new component would provide the “meaningful indicators” of success that Chairman Wheeler stated industry should provide. Referring to this recommendation, the Public Notice asks what measures the CSAR should include to provide appropriate levels of visibility about the state of cybersecurity risk management.²¹ The Report explains that the most “meaningful indicators” of success regarding the communications sector’s risk management practices would be “measurable outcomes” or “outcome-based measures” relating to the “availability of the critical infrastructure to deliver critical services.”²²

²⁰ Report at 7.

²¹ Public Notice at 2.

²² Report at 25, 28.

Such indicators would include information about cyber threat trends that will help industry focus on preventive measures and ensure the availability of networks to deliver critical services. By using forward-looking indicators, industry will be able to understand how threats change over time so that industry can anticipate and prevent them. Because attack vectors vary depending on industry sector and the size of the business, the indicators of success may well vary for different industry segments, as well as for companies of different sizes within each segment. This approach will put industry on a proactive, rather than reactive, footing and will help the telecommunications industry identify other industry sectors that need immediate attention, particularly those industries that may lack experience with, and appreciation of, cybersecurity threats.

By contrast, the use of backward-looking data, such as the number of botnets a company has identified or distributed denial of service (“DDoS”) attacks a company has addressed, would not provide a useful means of assessing cybersecurity risk management and would not enable industry to focus on preventative measures. As the Report acknowledges, data points of this sort are not outcome-based measures and provide no insight into network availability.²³

The Commission should reaffirm the Report’s conception of meaningful indicators of successful cybersecurity risk management and work with industry and DHS (and other governmental counterparts, where appropriate) to ensure that industry uses forward-looking measurements to assess risk management in this area.

²³ Report at 28.

C. Active participation in DHS C³ program

Finally, the Report recommends “[a]ctive and dedicated” participation in DHS’s Critical Infrastructure Cyber Community C³ Voluntary Program.”²⁴ CTIA believes that DHS’s C³ program could be a particularly useful resource for smaller companies that may lack the requisite level of sophistication about cybersecurity issues. For instance, the C³ program could develop and disseminate practical “how to” guidance and provide resources, guidelines, and instructions to small companies that lack access to such materials.

The C³ program also has potential to provide other benefits to industry. For instance, because the C³ program is not limited to any one industry sector, it has the ability to offer cross-industry guidance on cybersecurity matters. In addition, because DHS oversees the program, companies can participate in classified meetings that will protect sensitive information. Industry also has a role to play in the C³ program, and CTIA members look forward to participating in this education and outreach process to leverage the work of CSRIC IV.

IV. THE COMMISSION SHOULD FOCUS ON PROVIDING PRACTICAL ADVICE FOR OVERCOMING BARRIERS TO THE EFFECTIVE APPLICATION OF THE CSRIV IV RECOMMENDATIONS

Finally, the Public Notice seeks comment about barriers to implementing the Report’s recommended voluntary mechanisms, the degree to which the barriers may change based on other factors, and what can be done to address such barriers.²⁵ The Report already includes a detailed assessment of the various challenges to implementing the Framework, including financial, legal, technological, consumer/market, and operational barriers for different industry

²⁴ Report at 6.

²⁵ Public Notice at 2.

segments.²⁶ CTIA members thus do not go into detail about those barriers here, but instead focus on how the Commission could help devise ways to overcome them.

Industry may benefit from practical guidance on how to overcome potential barriers. For example, companies have access to an abundance of technological tools that they can use to meet cybersecurity goals, but it can be difficult to determine which tool to use. For instance, as the Report notes, it is difficult to assess the return on investment for any one particular technical tool, and it is particularly so for smaller and medium-sized companies, which may view the costs of implementing the Framework as offering no “calculable” return at all.²⁷ Such companies would benefit from guidance regarding how to assess, and calculate the cost of, their options. In addition, from an operational perspective, it is hard for some companies to match their assets against an appropriate risk model. Such companies risk adopting overly broad and expensive solutions. If the burdens imposed on smaller companies are too great, cybersecurity risk for these companies could actually increase. Companies could benefit from guidance in this area, as well.

As the Report recommends, appropriate government agencies should focus going forward on providing flexible examples regarding how companies could make these difficult decisions. The C³ program, discussed above, would be one logical resource for such information. The Commission also potentially could add value through its own outreach efforts. The Commission should refrain, however, from attempting to prescribe guidance or rules for making decisions. Indeed, government agencies are not in a position to dictate how companies should make their risk management assessments, and doing so would contravene Chairman Wheeler’s and the

²⁶ See generally Report, Section 9.6, at 202-320.

²⁷ Report at 204.

Report's shared, strong preference for a non-regulatory approach over any sort of prescriptive regime.²⁸

V. CONCLUSION

CTIA strongly supports the Report's comprehensive and scalable recommendations for implementing the NIST Framework. These recommendations will advance the Commission's cybersecurity goals and can serve as a model for other industry sectors as they develop plans to put the NIST Framework into effect. The Commission can best support industry's implementation of the Report's recommendations by leveraging the work of CSRIC IV for use by other industry sectors; fostering communication and cooperation with its international counterparts; encouraging involvement in the process beyond critical infrastructure companies; ensuring that the Report's voluntary mechanisms are effective; encouraging the use of meaningful, forward-looking indicators to measure successful cybersecurity risk management; and participating in outreach and education efforts. CTIA and its members look forward to continuing to work with the Commission, as industry and other stakeholders implement the various measures that the Report recommends.

Respectfully submitted,

/Thomas Power/
Thomas Power
Senior Vice President, General Counsel

/Thomas Sawanobori/
Thomas Sawanobori
Senior Vice President, Chief Technology Officer

CTIA – THE WIRELESS ASSOCIATION®
1400 16th Street, NW, Suite 600

²⁸ Report at 4.

Washington, DC 20036
(202) 736-3200

May 29, 2015