Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC20554

In the Matter of	)	
	)	
FCC'S Public Safety and Homeland Security Bureau Requests Comment on CSRIC IV Cybersecurity Risk Management and Assurance Recommendations	)	PS Docket No. 15-68

COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

I. INTRODUCTION AND SUMMARY

The Telecommunications Industry Association ("TIA") hereby submits comments in response to the Federal Communications Commission's ("Commission") Public Notice[1] seeking comment on the report on Cybersecurity Risk Management and Best Practices submitted by the fourth Communications Security, Reliability and Interoperability Council ("CSRIC") IV, specifically its report that includes segment-specific analysis of the application of the Cybersecurity Framework.[2]

TIA represents hundreds of information and communications technology ("ICT") manufacturer, vendor, and supplier companies in government affairs and standards

---

[1] *FCC'S Public Safety and Homeland Security Bureau Requests Comment on CSRIC IV Cybersecurity Risk Management and Assurance Recommendations*, Public Notice, PS Docket No. 15-68 (rel. Mar. 19, 2015) ("PN").

[2] *See* CSRIC IV, "Cybersecurity Risk Management and Best Practices, Working Group 4: Final Report (adopted Mar. 18, 2015), *available at* http://transition.fcc.gov/pshs/advisory/csric4/CSRIC_WG4_Report_Final_March_18_2015.pdf ("CSRIC WG 4 Report").

development. Numerous TIA members are companies producing ICT products and systems, creating information security-related technologies, and providing ICT services information systems, or components of information systems. These products and services innovatively serve many of the critical infrastructure sectors directly impacted by President's Executive Order[3], which created the *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0* on which the Communications Security, Reliability, and Interoperability Council's Working Group 4 ("WG 4") best practices and recommendations are based.[4] Representing our membership's commitments in this area, TIA holds membership and is actively engaged in key public-private efforts that contribute to secure information systems, including the CSRIC; the Communications Sector[5] and Information Technology Sector[6] Coordinating Councils; and the National Coordinating Center for Communications ("NCC"), the Information Sharing and Analysis Center ("ISAC") for telecommunications, part of the Department of Homeland Security's ("DHS") National Cybersecurity and Communications Integration Center;[7] among other successful public-private partnerships that the CSRIC WG 4 Report builds upon.

---

3 *See* Executive Order 13636 – Improving Critical Infrastructure Cybersecurity, rel. Feb. 12, 2013 ("EO").

4 The National Institute of Technology and Standards (NIST), *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0* (Feb. 12, 2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf ("NIST Cybersecurity Framework").

5 http://www.commscc.org/

6 http://www.it-scc.org/

7 http://www.dhs.gov/national-coordinating-center-communications

Through its Cybersecurity Working Group, TIA members engage in policy advocacy consistent with the following principles:

- Public-private partnerships should be utilized as effective vehicles for collaborating on current and emerging threats.
- Industry-driven best practices and global standards should be relied upon for the security of critical infrastructure.
- Voluntary private sector security standards should be used as non-mandated means to secure the ICT supply chain.
- Governments should provide more timely and detailed cyber intelligence to industry to help identify threats to protect private networks.
- Cybersecurity funding for federal research efforts should be prioritized.

We appreciate the CSRIC's efforts and transparent process in the application of the Cybersecurity Framework to communication critical infrastructure to date, and look forward to working with the Commission and other governmental stakeholders both directly and through the CSRIC's construct moving forward, and offer the specific input below based on the consensus views of TIA's hundreds of ICT manufacturer, vendor, and supplier member companies.

II. TIA SUPPORTS THE CSRIC IV CYBERSECURITY REPORT CONTAINING RECOMMENDATIONS AND BEST PRACTICES ON CYBERSECURITY RISK MANAGEMENT

In the PN, the Commission asks for input on the ways that the CSRIC IV recommendations are sufficient to meet the Commission's goal of reducing cybersecurity risk to critical infrastructure, enterprises, and consumers; and in what ways, if any, these recommendations might be improved, augmented, or made more specific.[8] TIA heavily participated in the process of the NIST Cybersecurity Framework's ("Framework") development, urging for the preservation of the flexibility and the ability to innovate, deference to successful public-private partnerships, and recognition of the necessity of international approaches and standards.[9] We believe that the Framework reflects these priorities, and will continue to work with NIST in further development of the Framework.

Since the Framework's release, there have been a number of proposals on how it should be used in different sectors. TIA agrees with the Framework's authors (NIST) and many others that the Framework is a voluntary means – based on existing standards, guidelines, and practices – for reducing cyber risks to critical infrastructure, which does not inform a mandatory or regulatory approach.

Building on this view, TIA was pleased to take a leadership role in the CSRIC Working Group 4 effort to craft guidance on how to secure communications critical infrastructure. TIA fully supports the recommendations in the CSRIC-approved and Commission-endorsed report,

---

[8] PN at 2.

[9] *See, e.g.*, Comments of TIA, *Developing a Framework to Improve Critical Infrastructure Cybersecurity* (Docket Number 130208119–3119–01), filed Apr. 8, 2013, *available at* http://www.tiaonline.org/sites/default/files/pages/TIA_Comments_NIST_Cybersecurity_Framework_040813.pdf.

Cybersecurity Risk Management and Best Practices, which thoroughly lays out voluntary mechanisms to provide macro-level assurance to the Commission and the public that communications providers are taking the necessary corporate and operational measures to manage cybersecurity risks across the enterprise through the application of the NIST Cybersecurity Framework (or an equivalent construct). The report is particularly beneficial in that it is scalable to the diversity of critical infrastructure communications sector stakeholders.

This report not only provides guidance to communications sector stakeholders, but also serves as a model for industry members and policymakers globally, and reinforces the success of the voluntary public-private partnership model which TIA and many others advocate as the most effective means to improve cybersecurity for critical infrastructure. In an increasing number of jurisdictions, where alternative mandate-based approaches are sometimes being proposed, TIA continues to emphasize to these governments that the most effective solutions ensure innovation by relying on voluntary use of internationally-accepted standards and best practices, and that neither the NIST Cybersecurity Framework nor any other government action should be used to implement cybersecurity policies that would restrict trade in ICT equipment imported to, or exported from, other countries that are part of the global trading system. TIA believes that the Commission should play a role in increasing awareness of the CSRIC's approach to cybersecurity risk management within the United States government (such as in the Cybersecurity Forum for Independent and Executive Branch Regulators[10]), as well as through government-to-government discussions and other international fora.

[10] *See* http://pbadupws.nrc.gov/docs/ML1501/ML15014A296.pdf.

Building on the above, TIA further notes its support for the voluntary mechanisms put forward by the Commission in the PN.[11] We believe that the CSRIC's cybersecurity recommendations contain guidance on the metrics component[12] that will be helpful in company-specific discussions on cybersecurity risk management, but defer to individual companies to provide the appropriate shape to such discussions. TIA also strongly urges for deference to the Communications Sector Coordinating Council as it works to shape its approach to this topic in adding a component to the Communications Sector Annual Report to address the state of cybersecurity risk management.

III. TIA SUPPORTS AND URGES FOR ENHANCED COMMISSION COORDINATION IN KEY AWARENESS AND EDUCATION EFFORTS IN SUPPORT OF THE CSRIC IV's VOLUNTARY APPROACH TO CYBERSECURITY RISK MANAGEMENT

TIA notes its support for enhanced coordination and partnership between the Commission and the Department of Homeland Security's ("DHS") Critical Infrastructure Cyber Community C3 Voluntary Program. Awareness of the Framework is a valuable and necessary step, and it is important that it be accompanied by a correct understanding of how to use the Framework. TIA has observed that not all stakeholders are fully aware of the voluntary nature of the NIST Cybersecurity Framework. For instance, TIA has observed several attempts by policymakers to make corporate use of the Framework mandatory, disregarding the nature of the Framework as a toolbox from which organizations may pull tools to aid in the development and/or enhancement of their particular cybersecurity programs as appropriate. We urge for adherence to the voluntary nature of the Framework prescribed in the EO, and that the

---

11 *See* PN at 2.

12 *See* CSRIC WG 4 Report at 355-369.

Commission partner with DHS in emphasizing that the EO requires the incorporation of voluntary consensus standards and industry best practices, along with the reasons for this approach (such as consistency with the Office of Management and Budget's Circular A-119[13] and the National Technology Transfer and Advancement Act[14]).

[13] *See* OMB Circular A-119 Revised, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities (rev. Feb. 10, 1998), *available at* http://www.whitehouse.gov/omb/rewrite/circulars/a119/a119.html.

[14] *See* 15 U.S.C. §3701 et seq. (1996).

IV. CONCLUSION

TIA appreciates the Commission's consultation regarding these possible rule revisions, and urges consideration of the recommendations above. We stand ready to work with the Commission on improving the cybersecurity of critical infrastructure.

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Brian Scarpelli
Director, Government Affairs

Avonne Bell
Sr. Manager, Government Affairs

David Gray
Manager, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1320 North Courthouse Rd.
Suite 200
Arlington, VA 22201
(703) 907-7700

Its Attorneys

May 29, 2015