

**Before the  
Federal Communications Commission  
Washington, D.C. 20554**

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

**COMMENTS OF MOTOROLA SOLUTIONS INC.**

Motorola Solutions Inc. (“Motorola Solutions”) hereby responds to the Federal Communications Commission’s request for comment on the Communications Security Reliability and Interoperability Council IV (“CSRIC IV”) Working Group 4 Report on cybersecurity risk management.<sup>1</sup>

**I. INTRODUCTION**

The report of the CSRIC IV Working Group 4 is both groundbreaking and substantial and should be used as a model for future efforts. It was developed by an engaged group of cybersecurity experts representing a wide cross-section of the communications industry and defines an evolving approach to cybersecurity. Motorola Solutions believes the Working Group 4 report moves in the direction of establishing a sustainable framework for evaluating and improving cybersecurity. The Report offers meaningful recommendations for further action to help ensure that the industry is adequately addressing cybersecurity risks, while also providing

---

<sup>1</sup> FCC’s Public Safety and Homeland Security Bureau Requests Comment on CSRIC IV Cybersecurity Risk Management and Assurance Recommendations, PS Docket No. 15-68, *Public Notice*, DA 15-354 (rel. March 16, 2015) (“Public Notice”). *See also* The Communications Security, Reliability and Interoperability Council IV, Working Group 4 Final Report, *Cybersecurity Risk Management and Best Practices* (March 2015) available at [http://transition.fcc.gov/pshs/advisory/csric4/CSRIC\\_WG4\\_Report\\_Final\\_March\\_18\\_2015.pdf](http://transition.fcc.gov/pshs/advisory/csric4/CSRIC_WG4_Report_Final_March_18_2015.pdf) (“Report”).

analytical frameworks and use cases to assist industry members in improving security within their enterprises. The Commission should be applauded for facilitating this effort and should now review the final reports closely and encourage their implementation.

**II. THE CSRIC IV WORKING GROUP 4 REPORT IS AN IMPORTANT ACCOMPLISHMENT FOR PROMOTING CYBERSECURITY RISK MANAGEMENT IN THE COMMUNICATIONS SECTOR.**

Motorola Solutions observed first hand CSRIC IV Working Group 4 to be a diverse, industry-led group of experts that benefited from close coordination with representatives of both Federal and State governments. As noted in the Report, the Working Group consisted of more than 100 cybersecurity professionals, divided into five industry segment subgroups and five topic area “feeder groups.”<sup>2</sup> The various groups collaborated to produce individual reports as well as the overall report and recommendations of the Working Group. Taken together, this output contains substantive analysis of cybersecurity practices in the sector and forward-looking recommendations tailored to the communications industries.

The final Working Group Report benefited greatly from the group being industry-led while including meaningful participation from Federal (*e.g.*, FCC, National Institute of Standards and Technology (“NIST”), Department of Homeland Security (“DHS”), Department of Health and Human Services (“HHS”) and state/local government (*e.g.*, Florida, Iowa, Nevada, and Pennsylvania) stakeholders.<sup>3</sup> This dynamic led to the successful result of the working group, which produced useful, actionable results that can improve overall security.

In its report, CSRIC IV Working Group 4 adapted the risk management approach of the NIST *Framework for Improving Critical Infrastructure Cybersecurity* version 1.0 (“NIST Cybersecurity Framework”) for application in the communications sector. As the Working

---

<sup>2</sup> Report at 4

<sup>3</sup> *Id.* at 16-18.

Group 4 Report recognized, this approach marked a “fundamental shift” from “the traditional multi-year CSRIC review cycles [that] can no longer keep pace with the accelerating deployment of new network and edge technologies across the ecosystem along with the rapid advancements in increasingly inexpensive, perishable, and more sophisticated cyber threats.”<sup>4</sup> In the NIST Cybersecurity Framework the “U.S. government has clearly endorsed development of a voluntary, risk-based model that enables organizations to prioritize and implement solutions based on informed, enterprise-tailored, business-driven considerations,”<sup>5</sup> and the Working Group 4 Report carried that work onward, customizing it for the communications sector.

The CSRIC WG 4 report provides an analytical framework and numerous use cases to assist communications companies throughout the sector in adapting the NIST Cybersecurity Framework for application in their own enterprises. Adopting the Framework’s emphasis on “critical infrastructure,” each industry segment subgroup evaluated the architectural components of their communications systems, made scoping determinations about critical elements, and analyzed the risk management functions, categories, and subcategories developed by NIST in the context of their own segments. While the top-level report includes specific finding, conclusions, and recommendations relevant to the entire industry, each segment report stands as a roadmap for companies seeking to bring the risk management principles of the NIST Cybersecurity Framework to bear to protect their own systems.

The Working Group 4 Report recognizes that a one-size-fits-all approach to cybersecurity will not be effective and that improving cybersecurity risk management is a holistic undertaking cutting across multiple industries. As illustrated in the reports of the Cyber Ecosystem and Dependencies subgroup, in which Motorola Solutions participated, and the other feeder groups,

---

<sup>4</sup> *Id.* at 11.

<sup>5</sup> *Id.*

cybersecurity risk management is the responsibility of entities in all communications segments and across the Internet ecosystem, including different sized enterprises, and entities at different points in the service delivery chain. Because of these broad cross-sector dependencies, the report illustrates that cybersecurity relies upon a diverse ecosystem that cannot be fully ensured by any one party, industry, or regulator. Therefore, non-regulatory approaches that bring diverse parties together to share information and strategies, such as CSRIC IV Working Group 4, the DHS Critical Infrastructure Cyber Community (C<sup>3</sup>) Voluntary Program, and established efforts at various industry-led and technical forums, are the best mechanisms for continuing to build cybersecurity capacity.

### **III. THE CSRIC WG 4 REPORT OFFERS SOUND RECOMMENDATIONS TO INDUSTRY AND GOVERNMENT STAKEHOLDERS.**

Working Group 4 was tasked with recommending “voluntary mechanisms to provide macro-level assurance that communications providers (*i.e.*, broadcast, cable, satellite, wireless, and wireline) are taking the necessary corporate and operational measures to manage cybersecurity risks across their enterprise.”<sup>6</sup> In doing so, the Working Group developed recommendations directed both to industry members and to regulators that are flexible enough to be adapted to the individual needs of each enterprise or industry segment. Consistent with the NIST Framework, and embodying the “new paradigm” approach set forth by Chairman Wheeler,<sup>7</sup> the report recommends voluntary processes and assurances, not new regulatory obligations and enforcement mechanisms.

---

<sup>6</sup> See CSRIC IV Working Group Descriptions and Leadership, at 5 <http://transition.fcc.gov/bureaus/pshs/advisory/csric4/CSRIC%20IV%20Working%20Group%20Descriptions%2010%2023%2014.pdf>.

<sup>7</sup> Remarks of FCC Chairman Tom Wheeler, American Enterprise Institute (Jun. 12, 2014), available at [https://apps.fcc.gov/edocs\\_public/attachmatch/DOC-327591A1.pdf](https://apps.fcc.gov/edocs_public/attachmatch/DOC-327591A1.pdf).

The voluntary mechanisms identified by the report strike an appropriate balance between providing assurance and protecting proprietary and confidential data, while also reflecting the diversity of industry and government parties with a stake in improving cybersecurity risk management. In addition to making recommendations for Commission activities in the cybersecurity arena, the report recognizes the central importance of continued engagement with DHS, which, as the Sector Specific Agency for communications, is tasked with developing and implementing the sector specific plan for critical infrastructure protection in the communications sector. Each of the three new voluntary mechanisms call for collaboration between the agencies, underscoring the holistic, non-regulatory approach needed in this area.

The Working Group 4 Report calls for the development of a voluntary program for confidential meetings among the Commission, DHS, and specific companies.<sup>8</sup> The meetings will give the Commission insight into the practices of individual companies and recent developments in industry. The usefulness of these reports depends upon their confidentiality and their remaining outside the regulatory context. In particular, to facilitate the transparency and dialogue intended for these sessions, companies must feel secure that the information they share shall be covered under the Protected Critical Infrastructure Information (“PCII”) Program and shall not be divulged, disclosed, or used against them in a future enforcement proceeding.

The Working Group 4 Report also proposes a new component of the Communications Sector Annual Report, which will provide a segment-level snapshot of risk management practices being deployed in the industry.<sup>9</sup> This report would be delivered to DHS through the Communications Sector Coordinating Council, and would be shared with the Commission through the Government Coordinating Council. Developing this report through the CSCC is

---

<sup>8</sup> Report at 7.

<sup>9</sup> *Id.*

seen as affording stronger confidentiality protection to communications companies, through their role as critical infrastructure providers, which will in turn provide additional comfort in sharing this data. Aggregating anonymized data from across the industry, this new section of the report will offer greater detail on threats and responses than has previously available to the Commission, and will aid it substantially in understanding industry trends and processes.

Finally, the Report recommends continued and expanded industry participation in the DHS C<sup>3</sup> Program.<sup>10</sup> C<sup>3</sup> already has proven an effective mechanism for spreading awareness of best practices and resources available for sector members to better manage cybersecurity risk. While the individual company meetings and sector-level report will improve the Commission's and other agencies' visibility into industry cybersecurity risk management practices, C<sup>3</sup> will provide a platform for promoting implementation of the NIST Framework across the sector.

The Working Group 4 Report and segment subgroup reports also offer numerous useful recommendations to companies throughout the communications ecosystem, going beyond the three mechanisms on which the FCC sought specific comment. As Working Group 4 explained, these reports “provide[] a valuable roadmap for companies in our sector to validate their existing risk management processes and/or enhance their capabilities based on an ongoing evaluation of their threats, vulnerabilities, and risk tolerance.”<sup>11</sup> The report offers guidance for how companies in the communications sector might analyze the NIST Framework and prioritize implementation of the risk management categories and subcategories in their enterprises. The reports recommend companies review internal governance and communications mechanisms to ensure risk management practices are integrated throughout, identifying numerous documents, best practices, and other informative references to assist companies in these tasks. By providing

---

<sup>10</sup> *Id.*

<sup>11</sup> *Id.* at 12.

analytical frameworks and illustrative use cases specific to each industry segment, the segment subgroup report can help industry members begin the process of applying the important risk management principles of the NIST Cybersecurity Framework to their own operations.

#### **IV. CONCLUSION**

Motorola Solutions appreciates the opportunity to have participated in the CSRIC Working Group 4 effort. The final reports are the product of the collective intelligence of an impressive cross-section of the communications industry. The Commission should review closely the findings and conclusions of the report, and should encourage the prompt implementation of the report's recommendations.

/s/ Chuck Powers

Chuck Powers  
Director, Engineering and Technology Policy

/s/ Mike Alagna

Mike Alagna  
Director, Homeland Security Strategic Initiatives  
and Policy

/s/ Catherine Seidel

Catherine Seidel  
Chief – Global Spectrum and Regulatory Policy

Motorola Solutions, Inc.  
1455 Pennsylvania Avenue, N.W.  
Washington, DC 20004  
(202) 371-6900

May 29, 2015