Resolution on Risk Management and Best Practices for Cybersecurity for Communications Providers: CSRIC IV Recommendations

WHEREAS, The cybersecurity risks to critical infrastructure industries and sectors regulated by State Commissions continue to increase and evolve in their persistence and sophistication; *and*

WHEREAS, In recent years, much of the cybersecurity focus of State Commissions has been on oversight of regulated utilities in the energy sector; specifically, the security of the high-voltage bulk electric system (BES), and local distribution systems for electric power; *and*

WHEREAS, The communications sector is also experiencing an increasing trend of cybersecurity threats; *and*

WHEREAS, Due to the interconnected nature to other vital critical infrastructure industries such as water and wastewater, natural gas, and electricity supply and delivery, as well as E-911 services and universal service programs, and to offer uninterrupted commercial service to its customers, the communications sector is increasing its efforts to address these threats and improve enterprise-wide risk management practices; *and*

WHEREAS, The Chairman of the Federal Communications Commission (FCC), Tom Wheeler, has made cybersecurity a high priority at the agency and has publicly called for greater voluntary efforts by communications providers, and has asked the Working Group 4 (WG 4) of the Communications, Security, Reliability and Interoperability Council (CSRIC), the key advisory council to the FCC on such matters, to address cybersecurity in a timely and effective way; *and*

WHEREAS, WG 4 worked diligently, with over 100 volunteer members, over the past 12 to 18 months to analyze these issues and develop key recommendations, which culminated in a Final Report that was adopted unanimously in March 2015; *and*

WHEREAS, The scope of WG 4's Final Report included the five industry segments that could be subject to attack and intrusion from malicious actors: broadcast; cable; satellite; wireless; and wireline; *and*

WHEREAS, The WG 4 Report used the National Institute of Standards and Technology (NIST) Framework for risk management of cybersecurity threats as its fundamental basis and provided specific guidance to individual companies on analytical tools and methods in applying the Framework; *and*

WHEREAS, The WG 4 Report also relied heavily on five feeder groups that worked to develop specific recommendations by sector and fed them up in to the larger group, namely: cyber ecosystems and dependencies, top threats and vectors, NIST Framework requirements and barriers, small and medium business, and measurements; *and*

WHEREAS, The WG 4 Report stressed the interdependencies of the communications sector to other vital critical infrastructure industries and highlighted the need for such sectors to coordinate their activities toward common threats through the use of the NIST Framework and other methods; *and*

WHEREAS, The final Report concluded that voluntary mechanisms of the industry were the most appropriate way to proceed, which includes FCC-initiated confidential company-specific meetings, a new component of the Communications Report that highlights cybersecurity risk management, and an increase in participation in the U.S. Department of Homeland Security's (DHS) Critical Infrastructure Cyber Community C^3 Voluntary Program; *and*

WHEREAS, Although some jurisdictional issues over cybersecurity and information sharing remain ambiguous without new federal legislation, most State Commissions, or similar State agencies, retain jurisdiction per State law and rules to ensure a reliable and secure communications system, especially for emergency communications services such as existing and next-generation 911 services, and many State Commissioners are also responsible for ensuring safety and reliability in the energy and water sectors, which are increasingly dependent on communications networks to operate their systems, and therefore have a strong interest in ensuring that communications providers in their States follow the best risk management practices for cybersecurity; *and*

WHEREAS, The WG4 members recognized that the cybersecurity threats and challenges are sophisticated, dynamic, and constantly evolving and therefore need constant attention, specifically stating: "While this WG4 CSRIC report represents a major milestone, the WG4 members acknowledge that we are not at the finish line."; *now, therefore be it*

RESOLVED, That the Board of Directors of the National Association of Regulatory Utility Commissioners, convened at its 2015 Summer Meetings in New York, New York, commends the broad participation and excellent work of members of the CSRIC Working Group 4 and its Final Report adopted in March 2015 to enhance cybersecurity risk management in the communications sector; *and be it further*

RESOLVED, That NARUC broadly endorses the analysis, findings, and recommendations included in the Final Report, including the new voluntary mechanisms for sharing confidential information on critical infrastructure through meetings initiated by the FCC, and urges that agency, DHS, and other federal agencies to cooperate in developing efficient and timely mechanisms to share such confidential information with State Commissions and other relevant State agencies in an appropriate way; *and be it further*

RESOLVED, That NARUC encourages State Commissions to engage actively and early with communications service providers in their States on cybersecurity practices, including through workshops, best practice sharing, or other proceedings consistent with State law and practice, and urges the use of the flexible risk management methodology of the NIST Framework, including the priority practices suggested in the small and medium business feeder group report, as initial steps easier to implement, and to the extent allowed by State law, to engage with communications providers in full information sharing, including confidential information, in parallel with the FCC-initiated efforts so that duplication and overlap are avoided to the extent possible; *and be it further*

RESOLVED, That NARUC commends Chairman Wheeler and the Bureau of Public Safety and Homeland Security for their leadership in cybersecurity, and look forward to continuing to work on these important issues of shared responsibility between States and federal agencies.

Sponsored by the Committee on Telecommunications and the Committee on Critical Infrastructure
Recommended by the NARUC Board of Directors, July 15, 2015