

**BEFORE THE PUBLIC SERVICE COMMISSION
OF THE STATE OF MISSOURI**

In the Matter of a Working Case to Address)	
Security Practices for Protecting Essential)	Case No. AW-2015-0206
Utility Infrastructure)	

AT&T'S RESPONSE

AT&T¹ respectfully opposes Missouri Public Service Commission Staff's June 8, 2015, Request for Commission Order and its July 17, 2015, Amended Request as the requests relate to the telecommunications industry.

AT&T commends the Commission and Staff on establishing a working case to address concerns about cybersecurity and physical security threats to utility infrastructure in Missouri. However, AT&T opposes the mandatory inclusion of the telecommunications industry in this effort because, by its very nature, the telecommunications industry is national in scope and these critical security issues are being extensively addressed at the federal level.² Requiring the telecommunications industry to participate in the current proceeding will add an additional layer of state activity that could result in duplicative, inconsistent, or irreconcilable requirements and will distract limited industry resources. Instead, AT&T recommends the Commission indicate that the responses to Staff's cybersecurity questions are optional and voluntary for telecommunications companies and that any information shared will be protected from public disclosure.

Missouri Proceedings. AT&T concurs with the Small Telephone Company Group ("STCG") that no "consensus" existed within the telecommunications industry to be included as

¹ Southwestern Bell Telephone Company, d/b/a AT&T Missouri, AT&T Corp., and Teleport Communications America, LLC will be referred to in this pleading as "AT&T."

² Numerous agencies currently have cybersecurity-related initiatives underway at the federal level, including the Federal Communications Commission ("FCC"), the Department of Homeland Security ("DHS"), the Department of Defense, National Telecommunications and Information Administration ("NTIA"), and the National Institute for Standards and Technology ("NIST").

respondents to a set of questions relating to cybersecurity and physical security issues. Like STCG, AT&T did not attend the March 23, 2015 Workshop as it understood the proceeding to involve Missouri's regulated electric, natural gas, sewer and water utilities. Subsequently, the President of the Missouri Telecommunications Industry Association ("MTIA") sent Staff written comments stating the MTIA's belief that telecommunications providers should not be included in this docket, explaining the FCC already has established a proceeding to address cybersecurity issues³.

Federal Proceedings. On February 12, 2013, President Obama issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," which set in motion a wide range of government initiatives designed to advance the nation's cybersecurity resiliency.⁴ That Order assigned the National Institute of Standards and Technology ("NIST"), an agency of the U.S. Department of Commerce, to lead the development of a "Cybersecurity Framework" to reduce cyber risks to critical infrastructure. Giving NIST a list of what should be included in the final Framework and one year to complete its work, the Order gave explicit instructions regarding the characteristics of the Framework and how it was to be used:

The Cybersecurity Framework shall provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk. The Cybersecurity Framework shall focus on identifying cross-sector security standards and guidelines applicable to critical infrastructure. The Cybersecurity Framework will also identify areas for improvement that should be addressed through future collaboration with particular sectors and standards developing organizations. To enable technical innovation and account for organizational differences, the Cybersecurity Framework will provide guidance that is technology neutral and that enables critical infrastructure sectors to benefit from a competitive market for products and services that meet the standards, methodologies, procedures, and processes developed to address cyber risks. The Cybersecurity Framework shall include guidance for measuring the performance of an entity in implementing the Cybersecurity Framework.⁵

³ See Response of the Missouri Small Telephone Company Group, and the Missouri Independent Telephone Company Group filed July 24, 2015, in Case No. AW-2015-0206, at p. 2.

⁴ Exec. Order No. 13,636, Improving Critical Infrastructure Cybersecurity, 78 FR 11737 (Feb. 19, 2013).

⁵ *Id.* at §7: Baseline Framework to Reduce Cyber Risk to Critical Infrastructure.

On February 12, 2014, NIST released the Framework for Improving Critical Infrastructure Version 1.0 stating that it “...enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure.”⁶ In sum, the Framework, which was a result of close collaboration between the public and private sectors, is a compendium of industry best practices and security standards available for voluntary use by critical infrastructure owners and operators.

The Framework initiative was aligned with the efforts of the FCC’s Communications Security Reliability and Interoperability Council (“CSRIC”) IV⁷, with the FCC indicating that CSRIC IV Working Group 4 should begin work immediately following the February 2014 release of the Framework because industry was a significant contributor of resources to the multi-stakeholder collaborative process that was being coordinated by NIST.⁸

On March 18, 2015, following an effort by over 100 cybersecurity experts from the communications sector, federal government, state government, equipment manufacturers, cybersecurity solution providers, and the financial, banking, and energy sectors, CSRIC IV unanimously adopted a detailed report that includes segment-specific analysis of the application of the Cybersecurity Framework as well as recommendations in response to the Commission’s charge. AT&T was actively engaged in the CSRIC IV process and preparation of the Working Group 4 Report. The CSRIC IV 415- page “Cybersecurity Risk Management and Best Practices, Working

⁶ National Institute of Standards and Technology, *Cybersecurity Framework - Workshops and Events*, <http://www.nist.gov/cyberframework/cybersecurity-framework-events.cfm> at 1.

⁷ CSRIC is a federal advisory committee composed of leaders from the private sector, academia, engineering, consumer/community/non-profit organizations, and government partners from tribal, state, local and federal agencies. The CSRIC IV charter called for an update of the cybersecurity best practices that had been developed as part of CSRIC II Working Group 2A: Cyber Security Best Practices. (That effort ended in March 2011 and produced 397 best practices covering a wide range of technology platforms and services. Federal Communications Commission, The Communications Security, Reliability and Interoperability Council II, *Working Group 2A Cybersecurity Best Practices – Final Report* (2011), available at <http://transition.fcc.gov/pshs/docs/csric/WG2A-Cyber-Security-Best-Practices-Final-Report.pdf>.

⁸ Cybersecurity Risk Management and Best Practices, Working Group 4: Final Report, p. 14.

Group 4: Final Report” (the “Working Group 4 Report”) is available on the FCC’s web site at: http://transition.fcc.gov/pshs/advisory/csrc4/CSRIC_WG4_Report_Final_March_18_2015.pdf

On March 19, 2015, the FCC’s Public Safety and Homeland Security Bureau issued a notice seeking comment on the Report, which CSRIC IV filed in PS Docket No. 15-68. (See attached Public Notice.) The FCC recently completed its comment cycle on the Report, with initial comments filed on May 29, 2015 and reply comments filed on June 26, 2015.

Security Concerns. The Commission should note that the Working Group 4 report recommends any meetings between the communications industry and the FCC be conducted under DHS’s Protected Critical Infrastructure Information (PCII) program, or a legally sustainable equivalent, which ensures, among other things, that the information shared is protected from public disclosure to avoid creating a roadmap for cyber criminals. This recommendation aligns with the Commission’s *Order* in Case No. EW-2013-0011, which appears to prohibit the type of written responses contemplated in Staff’s request:

No notifications or reports concerning the matters outlined in Staff’s recommendation shall be made in documentary form, i.e. no physical, digital or electronic reports shall be produced or filed in any docket, workshop, investigation or case, either noncontested or contested; nor shall the information provided to Staff be transmitted electronically to Staff or shared with any other entity. The information shall only be reported orally to designated Staff members, unless the Commission directs otherwise.⁹

Accordingly, the Commission should find that the responses to Staff’s cybersecurity questions are optional and voluntary for telecommunications companies and that any information they share will be protected from public disclosure.

The Commission’s Limited Jurisdiction. Modern communications networks function on a national and international scope. As the Working Group 4 Report makes plain, the

⁹ In the Matter of a Working Docket to Address Effective Cybersecurity Practices for Protecting Essential Electric Utility Infrastructure, Case No. EW-2013-0011, issued March 13, 2013 at p. 2.


communications industry now comprises many segments, including not only the traditional landline networks, but also the broadcast, cable, satellite and wireless segments as well. The Commission's regulatory oversight, however, is limited to a small subset of telecommunications providers (LECs), which in itself represents only a small part of today's communications and voice providers. As a result, information received from regulated LECs would have limited practical value. In addition, requiring LECs to provide responses (but not the other unregulated providers) to Staff's lengthy list of 21 questions creates an unfair regulatory burden on LECs.

CONCLUSION

The FCC and multiple other federal agencies are already comprehensively addressing Cybersecurity and physical security issues. The proposal to include telecommunications providers in any local Missouri Commission cybersecurity proceeding may result in duplicative, inconsistent, or irreconcilable requirements, cause security concerns and distract limited industry resources. Therefore, AT&T recommends the Commission indicate that the responses to Staff's cybersecurity questions are optional and voluntary for telecommunications companies, and that any information they share will be protected from public disclosure.

Respectfully submitted,

**SOUTHWESTERN BELL TELEPHONE
COMPANY, AT&T CORP., AND TELEPORT
COMMUNICATIONS AMERICA, LLC**

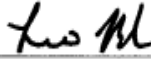
BY 

LEO J. BUB #34326

Attorney for Southwestern Bell Telephone
Company, d/b/a AT&T Missouri, AT&T Corp.,
and Teleport Communications America, LLC
909 Chestnut Street, Room 3558
St. Louis, Missouri 63101
314-235-2508 (telephone)/314-247-0014 (fax)
leo.bub@att.com

CERTIFICATE OF SERVICE

Copies of this document and all attachments thereto were served on the following by e-mail on July 27, 2015.



Leo J. Bub

General Counsel
Missouri Public Service Commission
P.O. Box 360
Jefferson City, MO 65102
gencounsel@psc.mo.gov

W.R. England III
Brian T. McCartney
Brydon, Swearngen & England P.C.
213 East Capital Avenue
Jefferson City, MO 65102
trip@brydonlaw.com
bmccartney@brydonlaw.com

Craig S. Johnson
Johnson & Sporleder
2420 Hyde Park Road, Suite C
Jefferson City, MO 65109
cj@cjaslaw.com

Dustin Allison
Office of the Public Counsel
P.O. Box 7800
Jefferson City, MO 65102
opcservice@ded.mo.gov

Missouri Cable Telecommunications
Association
Stephanie S. Bell
Blitz, Bardjett & Deutch, L.C.
308 East High Street, Suite 301
Jefferson City, MO 65101
sbell@bbdlc.com

MTIA
Richard Telthorst, CAE, President
312 East Capital Avenue
Jefferson City, MO 65102
ric@mtia.org