

**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 COMMENTS

AT&T¹ commends the Commission and its Staff on the valuable work invested in this case, particularly the tremendous amount of research, collaboration, and other efforts by Staff to produce its October 2, 2019, Follow-up Report on security practices for protecting essential utility infrastructure.

Pursuant to the Commission’s request for comment², AT&T continues to concur with Staff’s prior recommendation (originally made following its 2015 Workshop) against promulgating rules related to cybersecurity or infrastructure security “since utilities are actively engaged in [physical and cyber] security.”³ As subsequent utility company filings in this case and Staff’s new Follow-up Report reflect, this continues to hold true. With respect to the telecommunications industry, for example, which by its very nature is national in scope and mostly outside the Commission’s jurisdiction⁴, these important security issues are being extensively addressed at the federal level⁵ with active participation by all the major telecommunications companies that operate

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 Order Requesting Responses to Staff’s Follow-up Report, Case No. AW-2015-0206, issued October 2, 2019.

³ Staff Follow-up Report, p. 9 (brackets in original).

⁴ The communications industry now comprises many segments, including not only the traditional landline networks, but also the broadcast, cable, Internet, satellite and wireless segments as well. The Commission’s regulatory oversight, however, is limited to a small subset of telecommunications providers (LECs), which represents only a small part of today’s communications and voice providers.

⁵ 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”).

in the state. Adding an additional layer of state regulations could result in duplicative, inconsistent, or irreconcilable requirements and will distract limited industry resources from this critical and very sensitive area.

Instead, the Commission should continue to foster a collaborative public-private sector relationship that incentivizes continued investment and innovation in cyber and physical security practices and leverages the considerable resources currently available at the federal level. For example, the NIST “Framework for Improving Critical Infrastructure,”⁶ a close collaboration between the public and private sectors, has produced and maintains a compendium of industry best practices and security standards available for voluntary use by critical infrastructure owners and operators.⁷ This National Response Framework, led by FEMA as part of DHS, guides the Nation’s response to all types of disasters and emergencies. It is built on scalable, flexible, and adaptable concepts identified in the National Incident Management System to align key roles and responsibilities across the Nation. The Framework describes specific authorities and best practices for managing incidents that range from the serious but purely local to large-scale terrorist attacks or catastrophic natural disasters; the principles, roles and responsibilities, and coordinating structures for delivering the core capabilities required to respond to an incident; and how the response efforts integrate with those of the other mission areas.

In addition, the FCC’s Communications Security Reliability and Interoperability Council (“CSRIC”), consisting of over 100 cybersecurity experts from the communications sector, federal government, state government, equipment manufacturers, cybersecurity solution providers, and other industry sectors, aligns with the NIST Framework initiative and continually makes

⁶ President Obama’s Executive Order 13636 set in motion a wide range of government initiatives designed to advance the nation’s cybersecurity resiliency. It assigned 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. ⁶ Exec. Order No. 13,636, Improving Critical Infrastructure Cybersecurity, 78 FR 11737 (Feb. 19, 2013).

⁷ The NIST Framework can be accessed at: <https://www.nist.gov/cyberframework>

recommendations to the FCC to promote the security, reliability, and resiliency of the Nation’s communications systems.⁸ And DHS’ Cybersecurity and Infrastructure Security Agency (“CISA”) offers programs and services to help organizations better manage risk and increase resilience using all available resources, whether provided by the federal government, commercial vendors, or their own capabilities in various areas, including supply chain.⁹

Staff Recommendations

With respect to Staff’s Follow-up Report, AT&T respectfully offers the following comments and suggestions regarding specific Staff recommendations:¹⁰

Staff Recommendation No. 1 - Require each Missouri utility to identify, provide, and actively update contact information for both cyber and physical security points of contact. Points of contact should be personnel actively engaged with both cyber and physical security issues and not a member of the utilities’ counsel or involved with regulatory liaison activities.

AT&T Comment: AT&T has concerns that this recommendation will be unworkable for large telecommunications companies like AT&T, which operate on a global basis. AT&T, for example, employs over a thousand personnel in various groups across the company in multiple countries supporting such security and business continuity efforts for its various affiliates on an enterprise-wide basis. The organic movement of employees and responsibilities within these groups (e.g., through new hires, promotions, job transfers, creation of new positions or job functions, retirements, company reorganizations, and responsibility realignments) make a requirement to provide current contact information for “personnel with active responsibility for cyber and physical security” impracticable. Rather, AT&T’s local regulatory affairs director will be able to identify appropriate subject matter experts and coordinate meetings with the Commission or Staff when needed and is best suited to serve as Staff’s single point of contact for both cyber and physical security issues.

Staff Recommendation No. 2 - Require formal disclosure of plans specifically related to emergency response.

Staff Recommendation No. 3 - Require periodic Commission briefings on current security posture and related activities.

⁸ Information about CSRIC’s history, FCC charter, prior reports, current work efforts, and its best practices tool can be found on the FCC’s website at: <https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-vii>

⁹ CISA’s supply chain risk management initiatives can be accessed at: <https://www.dhs.gov/cisa/supply-chain-risk-management>

¹⁰ AT&T has limited its comments to the recommendations that would impact the telecommunications industry.

Staff Recommendation No. 4 - Require timely informal disclosure of both cyber and physical security incidents and any related response(s) and effect(s).

Staff Recommendation No. 5 - Specifically address supply chain risk management during periodic Commission briefings.

AT&T Comment: Formal disclosure (defined by the Staff Report as “in written form and presented to Commission Staff for review”¹¹) of utility emergency response, recovery and business continuity plans should be limited to non-proprietary materials that summarize the incident command structure the utility has in place to manage emergencies that impact the company’s business processes, assets or people. Such materials could, at a high level, generally describe the company’s emergency management operations, delineate its constituent entities, and the roles and responsibilities of those entities in restoring service and key business processes (e.g., technology operations, infrastructure, customer sales and service capabilities, provisioning, maintenance).

More detailed emergency response plans, current security posture, information relating to specific security incidents (both cyber and physical), the resulting responses, and assessments of specific risks (e.g., supply chain risks), however, should remain protected from public disclosure (intended or accidental) because of their high degree of sensitivity and to help avoid creating a roadmap for cyber and other criminals. The Commission correctly recognized the heightened need for the security of such information in its working case concerning practices for protecting essential electric utility infrastructure when it stated:

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.¹²

To the extent the Commission or Staff has a need for more detailed information, confidential briefing on an as-requested basis and not for public disclosure would provide more appropriate protection for such highly sensitive information. Mere informal disclosure (defined as “done verbally with commission Staff and would be the basis for further discussion and/or review of incident response, additional security measures and/or posture changes”¹³) alone may not provide the appropriate level of protection.

Staff Recommendation No. 10 - Encourage utilities to actively participate in the Intelligence Liaison Officer (ILO) program to receive pertinent threat information and provide information on

¹¹ Staff Follow-up Report, p. 14.

¹² 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. The Commission closed this case on March 5, 2015, and replaced it with the current working case, AW-2015-0206, to address general security issues for all utilities.

¹³ Staff Follow-up Report, p. 14.

suspicious activities that they may encounter in conducting everyday operations.

Staff Recommendation No. 11 - Proactively inform Missouri utilities about the Sensitive Compartmented Information Facility (SCIF) capabilities at the MIAC and the timing of any classified briefings that are taking place for cleared personnel.

Staff Recommendation No. 12 - Actively participate in the organization and development of a Utility Information Exchange Group and encourage all Missouri utilities to participate.

Staff Recommendation No. 13 - Actively participate in the improvement of information sharing between the public and private sectors by encouraging the involvement of investor-owned utilities, cooperative utilities, and municipal utilities where possible.

Staff Recommendation No. 21 - Encourage all utility owners and operators to engage the Department of Homeland Security (DHS) and the Missouri National Guard Cyber Team and leverage their respective resources.

AT&T Comment: AT&T supports the effort to foster a collaborative public-private sector relationship that incentivizes continued investment and innovation in cyber and physical security practices. To that end, AT&T recommends utilizing the considerable resources currently available at the federal level and avoid duplicating programs or processes that already exist. For example, DHS' Cyber Information Sharing and Collaboration Program ("CISCP") enables information exchange and the establishment of a community of trust between the Federal Government and critical infrastructure owners and operators, enabling the sharing of cyber threat, incident, and vulnerability information in near real-time to collaborate and better understand cyber threats. Through DHS's National Cybersecurity and Communications Integration Center ("NCCIC"), CISCP members can receive guidance on cyber-related threats to prevent, mitigate, or recover from cyber incidents.¹⁴

DHS' National Coordinating Center ("NCC") for telecommunications continuously monitors national and international incidents and events that may impact emergency communications (incidents include not only acts of terrorism, but also natural events such as tornadoes, floods, hurricanes, and earthquakes).¹⁵ The NCC partners with private industry members of the Communications Information Sharing and Analysis Center ("ISAC") and government organizations to facilitate the exchange of vulnerability, threat, intrusion, and anomaly information. ISACs are sector-specific (e.g., aviation, communications, energy, financial services), non-profit, member-driven organizations formed by critical infrastructure owners and operators to share information between

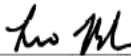
¹⁴ Information relating to CISP, its products and services can be accessed at: <https://www.cisa.gov/ciscp>

¹⁵ Information concerning the NCC, its functions, and industry and government partners can be accessed at: <https://www.cisa.gov/national-coordinating-center-communications>

government and industry. There is also a Multi-State ISAC (“MS-ISAC”) that provides services and information sharing to state, local, tribal, and territorial governments to help enhance their ability to prevent, protect against, respond to and recover from cyberattacks and compromises.¹⁶

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

1010 Pine Street, Room 19E-D-01

St. Louis, Missouri 63101

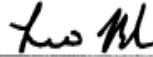
314-396-3679 (telephone)

leo.bub@att.com

¹⁶ Information concerning the MS-ISAC can be accessed at: <https://www.cisecurity.org/ms-isac/>

CERTIFICATE OF SERVICE

I certify that this document was filed in EFIS, with system notification sent to all parties of record. I further certify that a true and correct copy of this document has been sent by e-mail to the Commission Staff and the Office of the Public Counsel on November 1, 2019.



Leo J. Bub

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

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