BEFORE THE TENNESSEE PUBLIC UTILITY COMMISSION

NASHVILLE, TENNESSEE

IN RE:	)	
	)	
RULEMAKING TO PROMULGATE RULES FOR UTILITY CYBERSECURITY PLAN REPORTING AS REQUIRED UNDER TENN. CODE ANN. § 65-4-127	)	**DOCKET NO. 23-00001**

COMMENTS OF THE CONSUMER ADVOCATE DIVISION IN RESPONSE TO NOTICE OF OPEN DOCKET FOR FILING COMMENTS

The Consumer Advocate Division in the Office of the Tennessee Attorney General ("Consumer Advocate"), by and through counsel, and pursuant to Tenn. Code Ann. § 65-4-118, respectfully submits these comments in the response to the "Notice of Open Docket for Filing Comments" filed by the Tennessee Public Utility Commission ("TPUC" or "Commission") on January 20, 2023, in TPUC Docket No. 23-00001, *In re: Rulemaking to Promulgate Rules for Utility Cybersecurity Plan Reporting as Required under Tenn. Code Ann. § 65-4-127.*

The Consumer Advocate strongly supports the promulgation of the proposed rules. Considering the growing threat and increasing frequency of cyberattacks on utility infrastructure and technology, clear cybersecurity and accountability measures are in the best interest of both utilities and the consumers they serve. The proposed rules will assist in improving data protection and reliability of service. The Consumer Advocate offers only the following limited comments for consideration by the Commission.

TENN. COMP. R. & REGS. 1220-04-15-.01(2)

The definition of "Cybersecurity event" as proposed in the rulemaking filing currently reads as follows:

(2) Cybersecurity event – any unauthorized use, alteration, ransom, or destruction

> of electronic data involving a utility's information or operation technology systems; a cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery.

The definition, as drafted, might plausibly be interpreted as pertaining only to the protection of "data." However, the intent of the second clause seems to broaden the scope of the definition. The definition should explicitly include not only compromises of data, but any intrusion, such as a denial-of-service ("DoS") attack (as contemplated in the subsequent proposed section 1220-04-15-.04(1)(d)).

The Consumer Advocate would further make the following observations regarding grammatical clarity: Confusion could arise from the use of the term "cybersecurity event" within the definition of the term "Cybersecurity event," as occurs in the second clause. Additionally, if the term "utility" in the first clause is intended to be synonymous with the term "organization" in the second clause, the Consumer Advocate recommends use of the same term in each place.

TENN. COMP. R. & REGS. 1220-04-15-.01(3)

The definition of "Cybersecurity plan" as proposed in the rulemaking filing currently reads as follows:

> (3) Cybersecurity plan – a plan that provides for the protection of the utility's information technology and operational technology systems from unauthorized use, alteration, ransom, or destruction of electronic data.

In this definition, it is not clear that "protection" includes a utility's *response* to a "Cybersecurity event." Rather, a "Cybersecurity plan" might be taken as only the initial measures for protection prior to the occurrence of an event. The Consumer Advocate would suggest that "Cybersecurity plan" be defined to also include a utility's "response to any Cybersecurity event or suspected Cybersecurity event" as defined in the first subsection.

TENN. COMP. R. & REGS. 1220-04-15-.04(1)(c), (d)

Section 1220-04-15-.04(1)(d) as proposed in the rulemaking filing currently reads as follows:

> (1) By July 1st of each calendar year, all utilities shall submit an attestation that the utility has prepared and implemented a cybersecurity plan. At minimum, the attestation shall include:
>
> [...]
>
> (d) A statement indicating whether the utility has a plan for communicating a cybersecurity event that results in loss of service, financial harm, or breach of sensitive business or customer data. The statement should specify whether the plan includes notification to the Commission and utility customers[.]

Rather than an indication of "whether" the utility has a plan for communication, the Consumer Advocate recommends that the proposed rule require a utility to affirm that it *does* have a plan for notifying the Commission and its customers of a "cybersecurity event that results in loss of service, financial harm, or breach of sensitive business or customer data." Consistent with the purpose of the proposed rule, subsection (c), concerning cybersecurity training of utility personnel, could also be changed from an inquiry ("whether") to a directive ("shall").

TENN. COMP. R. & REGS. 1220-04-15-.06(1)

Section 1220-04-15-.06(1) as proposed in the rulemaking filing currently reads as follows:

> (1) If a utility experiences a cybersecurity event, it shall notify, both verbally and in writing, the Chair of the Commission or their designee within 48 hours of the utility's discovery of the cybersecurity event.

As drafted, this provision requires notice only to the Commission and only when a Cybersecurity event has actually occurred. The Consumer Advocate would recommend that notice also be required for suspected Cybersecurity events, and notice be required specifically to customers when a Cybersecurity event or suspected Cybersecurity event involves customer data or

reliability of service (as required in Section 1220-04-15-.04(1)(d)).

CONCLUSION

Utility cybersecurity is essential to the provision of reliable service to consumers and for the protection of consumer and utility data. The Consumer Advocate acknowledges and thanks the Commission for its action in the promulgation of these rules and for the opportunity to provide comment.

RESPECTFULLY SUBMITTED,

MASON C. RUSH (BPR No. 039471)
Assistant Attorney General
Office of the Tennessee Attorney General
Consumer Advocate Division
P.O. Box 20207
Nashville, Tennessee 37202-0207
Phone: (615) 741-2357
Email: mason.rush@ag.tn.gov