

BEFORE THE TENNESSEE PUBLIC UTILITY COMMISSION

NASHVILLE, TENNESSEE

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

**COMMENTS OF THE CONSUMER ADVOCATE DIVISION IN RESPONSE TO THE
PROPOSED RULES AS REVISED**

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 proposed rules, as revised. On March 20, 2023, the Tennessee Public Utility Commission (“TPUC” or the “Commission”) held a rulemaking hearing, 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 Commission has since considered all comments and made certain changes to the proposed rules and filed a *Notice of Open Docket for Filing Limited Comments* stating a due date of April 14, 2023.

As stated in its initial comments, the Consumer Advocate strongly supports the promulgation of the proposed rules as cybersecurity and accountability measures are in the best interest of both consumers and utilities. The Consumer Advocate offers the following limited additional comments for consideration by the Commission with regard notice requirements in the proposed rules, as revised.

I. Notice to the Commission

The proposed TENN. COMP. R. & REGS. 1220-4-15-.06, as revised, provides the

following: “All utilities shall electronically notify the Commission’s Executive Director of any incidents that result in disruption of service.”¹ The Consumer Advocate recommends that (1) the rule require notification of the Commission within a definite time frame after an incident, and (2) the rule require notification of incidents resulting in data breaches as well as disruptions of service.

A. Definite Time Frame for Providing Notice of Cybersecurity Incidents

Providing a definite time frame for notification to the Commission is necessary to ensure that the Commission is informed of cybersecurity incidents in a timely fashion and to remove any ambiguity in the rule as to the reporting obligations of utilities. This Commission’s original draft of TENN. COMP. R. & REGS. 1220-4-15-.06 would have required notice within 48-hours, as clearly stated.² As a possible alternative, a 72-hour requirement was suggested by all commenting utilities in response to the original draft— Chattanooga Gas Company,³ Atmos Energy Corporation and Piedmont Natural Gas Company, Inc.,⁴ and Tennessee American Water Company.⁵ Those comments note that 72 hours is the standard recommended by the American Gas Association⁶ and codified in the recent Cyber Incident Reporting for Critical Infrastructure Act of 2022 (“CIRCIA”).⁷ Regardless the exact number of hours or days the Commission chooses to allow, the Consumer Advocate submits that the rule should explicitly require that cybersecurity incidents be reported to the Commission with some urgency and within a relatively

¹ See *Notice of Open Docket for Filing Limited Comments*, TPUC Docket No. 23-00001 (Mar. 31, 2023).

² *Id.*

³ *Chattanooga Gas Company’s Comments*, at 6, TPUC Docket No. 23-00001 (Mar. 14, 2023).

⁴ *Comments of Atmos Energy Corporation and Piedmont Natural Gas Company, Inc.*, at 8, TPUC Docket No. 23-00001 (Mar. 15, 2023).

⁵ *Comments of Tennessee American Water Company in Response to Notice of Open Docket for Filing Comments*, at 10, TPUC Docket No. 23-00001 (Mar. 17, 2023). The industry standard 72-hour period was also recommended by Southwest Gas Corporation in the Nevada rulemaking docket discussed herein. See *Responses of Southwest Gas Corporation to Questions Presented in the Procedural Order*, at 5, PUCN Docket No. 22-09017 (Nov. 22, 2022) (available at [22463.pdf \(state.nv.us\)](#)).

⁶ See, e.g., *Comments of Atmos Energy Corporation and Piedmont Natural Gas Company, Inc.*, at 8, TPUC Docket No. 23-00001 (Mar. 15, 2023).

⁷ See Cyber Incident Reporting for Critical Infrastructure Act of 2022, 6 U.S.C. § 681b(a)(1)(A) (2022). “A covered entity that experiences a covered cyber incident shall report the covered cyber incident to the Agency not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred.”

brief period.

Provisions specifying a time frame (to a greater or lesser degree) for reporting cybersecurity incidents to commissions have been adopted in other jurisdictions where cybersecurity regulations are in place. For example, in Maryland, confirmed cybersecurity breaches must be reported “to a Commission-designated representative . . . no later than 1 business day after confirmation, unless prohibited or recommended by law enforcement to avoid compromising an investigation.”⁸ Though less definite, in Michigan, gas and electric utilities must report cybersecurity incidents to commission staff “[a]s soon as reasonably practicable” and prior to any public notification.⁹ Likewise, in Oklahoma, water, gas, and electric utilities are “required to report cybersecurity or infrastructure security events that affect customers *immediately* to the [Public Utility Division] Director or designee.”¹⁰ In its current cybersecurity rulemaking docket, the Regulatory Operations Staff of the Public Utilities Commission of Nevada has recommended the following language in its most recent draft regulation: “At the earliest practicable moment following the discovery of a cybersecurity incident, but not later than 4 hours after notification to CISA, a reporting utility shall notify the person designated by the Regulatory Operations Staff of the Commission of the cybersecurity incident.”¹¹

Thus, even where a definite time frame is not specified, utilities in the jurisdictions above are nonetheless under a clear obligation to promptly report cybersecurity incidents to their state utility commissions. This Commission’s proposed rule, as revised, is ambiguous as to when a utility must report a cybersecurity incident. The Consumer Advocate accordingly recommends that the proposed rule include a definite time frame by which a utility must notify the Commission following a cybersecurity incident. In addition to aiding the Commission in its role,

⁸ MD. CODE REGS. 20.06.01.05 (2022).

⁹ See MICH. ADMIN. CODE r. 460.2324(2) (2020) (applicable to natural gas utilities); MICH. ADMIN. CODE r. 460.3205(2) (2019) (applicable to electric utilities).

¹⁰ OKLA. ADMIN. CODE § 165:45-21-7(c) (2019) (emphasis added) (applicable to natural gas utilities). See also OKLA. ADMIN. CODE § 165:65-9-2(4) (2019) (applicable to water utilities); OKLA. ADMIN. CODE § 165:35-33-7(c) (2019) (applicable to electric utilities).

¹¹ *Regulatory Operations Staff’s Letter Responsive to Procedural Order No. 2*, at Attachment B, PUCN Docket No. 22-09017 (Mar. 2, 2023) (available at [24413.pdf \(state.nv.us\)](https://www.pucn.state.nv.us/24413.pdf)).

this would also enable utilities to implement appropriate measures and design cybersecurity plans in light of clear reporting obligations.

B. Notice of Data Breaches

The Consumer Advocate further suggests that the rule should explicitly apply not only to disruptions of service but also to data breaches. The proposed rule, as revised, unnecessarily narrows the scope of the notice requirements to incidents involving only “disruption of service.”¹² However, the Commission should also be apprised of any cybersecurity incidents that result in the unauthorized access to, or acquisition of, data that compromises the security or confidentiality of either the utility or the personal information of consumers. Such notice would not need to include any information or details that might potentially create a risk of further data compromise.

II. Notice to Consumers

The Consumer Advocate also submits that the rule should require notice, subsequent to the notification of the Commission, to affected consumers in instances where a cybersecurity incident results in a breach of data pertaining to personal information of the utility’s consumers. As cyber-attacks occur with increasing frequency across every industry, it is increasingly important that consumers be informed when their personal data is at risk. This is particularly important in the utility industry, where consumers receive service from their utilities of necessity and without choice.

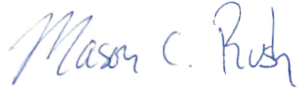
CONCLUSION

Utility cybersecurity is essential to the provision of reliable service to consumers and for the protection of consumer and utility data. As stated above, ensuring that the Commission and consumers receive the necessary notice of cybersecurity incidents is paramount to effective cybersecurity efforts. The Consumer Advocate acknowledges and thanks the Commission for its

¹² *Notice of Open Docket for Filing Limited Comments*, TPUC Docket No. 23-00001 (Mar. 31, 2023).

action in the promulgation of the proposed 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