BEFORE THE TENNESSEE PUBLIC UTILITY COMMISSION

NASHVILLE, TENNESSEE
May 24, 2023

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

ORDER APPROVING FINAL PROPOSED RULES FOR UTILITY CYBERSECURITY PLAN REPORTING

This matter came before the Tennessee Public Utility Commission with all Commissioners voting, during a regularly scheduled Commission Conference held on May 8, 2023, to consider the final proposed rules for reporting utility cybersecurity plans.[1]

On June 1, 2022, Public Chapter 1111 was signed into law and codified in Tenn. Code Ann. § 65-4-127. Starting July 1, 2023, the statute requires that every regulated electric, water, wastewater and natural gas utility is required to report and provide documentation to the Commission demonstrating that it has developed, implemented, and will maintain a cybersecurity plan. The purpose of this reporting requirement is to assure the Tennessee General Assembly and, by delegation, the Commission that a utility has taken appropriate measures to prevent, protect, and respond to a cybersecurity attack or incident against its facilities.

[1] Commissioner Kenneth C. Hill was absent from this Conference and did not vote in this matter.

During the regularly scheduled January 17, 2023 Commission Conference, the Commission voted to initiate a rulemaking proceeding to implement the cybersecurity plan reporting requirements of Tenn. Code Ann.§ 65-4-127. Also on that day, the Commission filed its Notice of Rulemaking Hearing with the Secretary of State with the proposed rules. On January 20, 2023, the Commission filed an additional Notice requesting comments on the proposed rules. The Commission received comments from the Consumer Advocate Division in the Office of the Tennessee Attorney General, a joint filing by Atmos Energy Corporation and Piedmont Natural Gas Company, Inc., Chattanooga Gas Company, and Tennessee-American Water Company.

On March 20, 2023, in accordance with the Notice of Rulemaking Hearing, the Commission held a public hearing on the proposed rules. Upon consideration of all comments received, the Commission published revised proposed rules for further comment on March 31, 2023. All parties that filed comments on the original proposed rules also filed comments on the revised proposed rules. The comments and information received greatly assisted the Commission in gaining new insight into how our regulated utilities approach cybersecurity. The commenters generally expressed concern that overly prescriptive filing requirements might create inconsistencies with various federal cybersecurity requirements, which these utilities are also subject to, leading to confusion and increased costs. The final proposed rule considered for approval and adoption addresses this concern and seeks to harmonize the Commission's rules with federal requirements, with the observation that federal guidance is evolving.

During the regularly scheduled Commission Conference held on May 8, 2023, the Commissioners considered the final proposed rules and voted unanimously to approve and

adopt the rules for the implementation of utility cybersecurity plan reporting. Staff was directed to proceed with the rulemaking process to resolution and final promulgation of the rules.

FOR THE TENNESSEE PUBLIC UTILITY COMMISSION:

Chairman Herbert H. Hilliard,
Vice Chairman David F. Jones,
Commissioner Robin L. Morrison,
Commissioner Clay R. Good,
Commissioner David Crowell, and
Commissioner John Hie concurring.

None dissenting.

ATTEST:

_____
Earl R. Taylor, Executive Director

Utility Cybersecurity Reporting Rules – Commission-approved on May 8, 2023

1220-04-15-.01 Definitions

(1) Commission – means the Tennessee Public Utility Commission.

(2) Cybersecurity incident - An event that, without lawful authority, jeopardizes, disrupts or otherwise impacts, or is reasonably likely to jeopardize, disrupt or otherwise impact, the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident on the system. This definition includes an event that is under investigation or evaluation by the Owner/Operator as a possible cybersecurity incident without final determination of the event's root cause or nature (such as malicious, suspicious, benign).

(3) Cybersecurity plan - a plan or plans intended to protect the utility's information technology and operational technology systems from unauthorized use, alteration, ransom, or destruction of electronic data.

(4) Information Technology System – means any services, equipment, or interconnected systems or subsystems of equipment that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange , transmission, or reception of data or information that fall within the responsibility of the Owner/Operator to operate and maintain.

(5) Operational Technology System – is a general term that encompasses several types of control systems, including industrial control systems, supervisory control and data acquisition systems, distributed control systems, and other control system configurations, such as programmable logic controllers, fire control systems, and physical access control systems, often found in the industrial sector and critical infrastructure. Such systems consist of combinations of programmable electrical, mechanical, hydraulic, pneumatic devices or systems that interact with the physical environment or manage devices that interact with the physical environment.

(6) Sworn Statement – means a written statement made under oath that the statement is true based on personal knowledge.

(7) Utility – a public utility defined by T.C.A. § 65-4-101 that provides electric, water, wastewater, or natural gas services.

Authority: T.C.A. §§ 65-2-102, 65-4-101, and 65-4-127.

1220-4-15-.02 Confidentiality

All documentation submitted in accordance with T.C.A. § 65-4-127 and these rules shall be treated as confidential and protected from public inspection. The Commission shall treat this documentation consistent with any federal laws, regulation or rule that protects sensitive security information or similarly designated information regarding cybersecurity.

Authority: T.C.A. §§ 65-2-102, 65-4-127, 10-7-504(a)(21)(i), and 10-7-504(a)(21)(C)(iii).

1220-4-15-.03 Cybersecurity Plan

(1) By July 1, 2023, or within one (1) year after a utility is formed, whichever is later, a utility shall prepare and implement a cybersecurity plan.

(2) Cybersecurity plans implemented in compliance with these rules must be assessed and updated by the utility no less frequently than once every two (2) years to address new threats.

Authority: T.C.A. §§ 65-2-102 and 65-4-127.

1220-4-15-.04 Annual Filing Requirements

(1) By July 1st of each calendar year, all utilities shall submit documentation that the utility has prepared and implemented a cybersecurity plan. At a minimum, the documentation shall include:

(a) Contact information for utility employee(s) responsible for cybersecurity;

(b) A statement indicating whether the utility conducts annual cybersecurity training for the utility personnel with access to any utility Information Technology System or Operational Technology System;

(c) A statement indicating whether the utility has procured cybersecurity insurance.

(2) The documentation filed must include a sworn statement by the utility's chief executive officer, president, or another person with an equivalent role and authority with respect to the cybersecurity plan. Such statement shall, at a minimum, confirm that the utility:

(a) Has prepared and implemented the cybersecurity plan described in the filing;

(b) The cybersecurity plan has been prepared or updated within the last two (2) years; and

(c) That all documentation and information filed is current and accurate.

Authority: T.C.A. §§ 65-2-102 and 65-4-127.

1220-4-15-.05 Failure to Comply; Sanctions

(1) A utility fails to comply with these rules, and is considered in non-compliance, when:

(a) The company does not file documentation required by these rules showing that it has prepared a cybersecurity plan by July 1st of each calendar year; and

(b) The company does not file documentation required by these rules showing that it has implemented that cybersecurity plan by July 1st of each calendar year.

(2) After hearing, the Commission may impose reasonable sanctions, including civil and monetary penalties, against a utility in non-compliance with these rules.

(3) Monetary penalties imposed by the Commission will be consistent with the statutory limit set in T.C.A. § 65-4-120.

(4) If the Commission determines that sanctions shall include a monetary penalty, it may

consider:

(a) The efforts the utility to comply with these rules;

(b) The financial stability of the utility; and

(c) The impact of noncompliance on customers of the utility.

(5) The Commission may require a utility to establish a separate fund to further support its compliance with these rules.

(6) Any utility in non-compliance shall be reported to the General Assembly in accordance with T.C.A. § 65-4-127(f).

Authority: T.C.A. §§ 65-2-102, 65-4-120, and 65-4-127.

1220-4-15-.06 Required Notification to Commission
A utility shall electronically notify the Commission's Executive Director of any cybersecurity incident that result in interruption of service within 72 hours after confirmation, unless prohibited or recommended by law enforcement to avoid compromising an investigation. In such event, notification shall be required within 24 hours after restriction is lifted by law enforcement.

Authority: T.C.A. §§ 65-2-102 and 65-4-127., and Tenn. R. & Regs. 1220-04-03-.42, 1220-04-04-.46, 1220-04-05-.36, and 1220-04-13-.12.

1220-4-15-.07 Cost Recovery for Cybersecurity Investment
(1) To the extent that costs related to action required by this rule are not already recovered in rates, the utility may seek cost recovery:

(a) By filing a petition pursuant to T.C.A. 65-5-103; or

(b) If permissible, by requesting an alternative regulatory mechanism pursuant to T.C.A. 65-5 103(d).

Authority: T.C.A. §§ 65-2-102, 65-4-127, and 65-5-103.