TENNESSEE PUBLIC UTILITY COMMISSION

Kelly Cashman-Grams
General Counsel
(615) 770-6856

Andrew Jackson State Office Bldg.
502 Deaderick Street, 4th Floor
Nashville, TN 37243-0001

NOTICE OF OPEN DOCKET FOR FILING LIMITED COMMENTS

DOCKET: **23-00001**

IN RE: ***In re Rulemaking to Promulgate Rules for Utility Cybersecurity Plan Reporting as Required under Tenn. Code Ann. § 65-4-127***

DATE: **March 31, 2023**

On March 20, 2023, the Tennessee Public Utility Commission ("Commission") held a public rulemaking hearing in the above-referenced docket to receive additional comments from the public on the proposed utility cybersecurity reporting rule. Since that time, the Commission has considered all the comments it has received, written and oral, and made certain changes to the proposed rules. Before final consideration by the Commissioners, the Commission welcomes additional feedback and comment on the proposed rule, *as revised*.

Any interested parties who wish to file written comments on the *revised* proposed rule may do so in the docket file. Attached to this notice is both a redline and clean copy version of the revised rule. The docket will remain open for comments until **2:00 p.m. on April 14, 2023**. Any questions concerning the rule should be directed to Jerry Kettles, Director of Policy at jerry.kettles@tn.gov or 615-770-6894 or to me at kelly.grams@tn.gov or 615-770-6856.

FOR THE TENNESSEE PUBLIC UTILITY COMMISSION:

Kelly Cashman Grams

Kelly Cashman Grams, General Counsel

cc: Docket File
TPUC Service List

1220-04-15-.01 Definitions
(1) Commission – means the Tennessee Public Utility Commission.

~~(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.~~

(~~3~~2) Cybersecurity plan - a plan or plans intended to protect ~~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.

~~(4) Information Technology - any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the utility. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.~~

(~~5~~3) Information Technology System ~~(IT 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.~~hardware and software related to electronic processing, and storage, retrieval, transmittal, and manipulation of data.~~

~~(6) Operational Technology - programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment) used to provide utility service. These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.~~

(~~7~~4) Operational Technology System ~~(OT 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.~~a system or network that monitors or controls electric, gas, wastewater or water system infrastructure used for utility operations.~~

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

(~~8~~6) 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 ~~an attestation~~ documentation that the utility has prepared and implemented a cybersecurity plan. At a minimum, the ~~attestation~~ documentation shall include:

~~(a) A summary of the program and procedures that describe the utility's approach to cybersecurity awareness and protection;~~

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

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

~~(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;~~

~~(e) A summary of any cybersecurity event during the reporting year that resulted in material loss of service, financial harm, or breach of sensitive business or customer data, including parties notified of the unauthorized action and remedial actions undertaken; and~~

(~~f~~c) A statement indicating whether the utility has procured cybersecurity insurance~~, and, if so, the current term and limits of such coverage~~.

(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 ~~affirm~~ 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 ~~of Cyber Event~~

All utilities shall electronically notify the Commission's Executive Director of any incidents that result in disruption of service.
~~(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.~~

~~(2) Within 30 days of the discovery of the cybersecurity event, the utility shall be available and prepared to brief the Chair of the Commission or their designee on the impact of the cybersecurity event to utility customers and on utility operations.~~

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.

1220-04-15-.01 Definitions
(1) Commission – means the Tennessee Public Utility Commission.

(2) 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.

(3) 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.

(4) 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.

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

(6) 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
All utilities shall electronically notify the Commission’s Executive Director of any incidents that result in disruption of service.

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.