

Department of State
Division of Publications
312 Rosa L. Parks Ave., 8th Floor, Snodgrass/TN Tower
Nashville, TN 37243
Phone: 615-741-2650
Email: publications.information@tn.gov

For Department of State Use Only

Sequence Number: 06-31-23
Rule ID(s): 9899
File Date: 6/27/2023
Effective Date: 9/25/2023

Rulemaking Hearing Rule(s) Filing Form

Rulemaking Hearing Rules are rules filed after and as a result of a rulemaking hearing (Tenn. Code Ann. § 4-5-205).

Pursuant to Tenn. Code Ann. § 4-5-229, any new fee or fee increase promulgated by state agency rule shall take effect on July 1, following the expiration of the ninety (90) day period as provided in § 4-5-207. This section shall not apply to rules that implement new fees or fee increases that are promulgated as emergency rules pursuant to § 4-5-208(a) and to subsequent rules that make permanent such emergency rules, as amended during the rulemaking process. In addition, this section shall not apply to state agencies that did not, during the preceding two (2) fiscal years, collect fees in an amount sufficient to pay the cost of operating the board, commission or entity in accordance with § 4-29-121(b).

Agency/Board/Commission:	Tennessee Public Utility Commission
Division:	Utilities/Legal
Contact Person:	Kelly Cashman-Grams, General Counsel
Address:	502 Deaderick Street, 4 th Floor, Nashville, TN 37243
Zip:	37243
Phone:	615-770-6856
Email:	Kelly.Grams@tn.gov

Revision Type (check all that apply):

<input type="checkbox"/> Amendment	<input type="checkbox"/> Content based on previous emergency rule filed on _____
<input checked="" type="checkbox"/> New	<input type="checkbox"/> Content is identical to the emergency rule
<input type="checkbox"/> Repeal	

Rule(s) (ALL chapters and rules contained in filing must be listed here. If needed, copy and paste additional tables to accommodate multiple chapters. Please make sure that **ALL** new rule and repealed rule numbers are listed in the chart below. Please enter only **ONE** Rule Number/Rule Title per row.)

Chapter Number	Chapter Title
1220-04-15	Utility Cybersecurity Plans & Reporting
Rule Number	Rule Title
1220-04-15-.01	Definitions
1220-04-15-.02	Confidentiality
1220-04-15-.03	Cybersecurity Plan
1220-04-15-.04	Annual Filing Requirements
1220-04-15-.05	Failure to Comply; Sanctions
1220-04-15-.06	Required Notification to the Commission of Cybersecurity Incident
1220-04-15-.07	Cost Recovery for Cybersecurity Investment

Place substance of rules and other info here. Please be sure to include a detailed explanation of the changes being made to the listed rule(s). Statutory authority must be given for each rule change. For information on formatting rules go to

<https://sos.tn.gov/products/division-publications/rulemaking-guidelines>.

1220-04-15-.01 DEFINITIONS

(1) Commission – 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 – 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 falls within the responsibility of the owner/operator to operate and maintain.

(5) Operational Technology System – 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 – 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.

1220-04-15-.02 CONFIDENTIALITY

All documentation submitted in accordance with T.C.A. § 65-4-127 and these rules shall be treated as confidential and shall not be open for public inspection. The Commission shall treat this documentation consistent with any federal law, 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)(A)(i), and 10-7-504(a)(21)(C)(iii).

1220-04-15-.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.

1220-04-15-.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; and
- (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, over the development and implementation of the cybersecurity plan. Such statement shall, at a minimum, confirm that:

- (a) The utility 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) All documentation and information filed is current and accurate.

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

1220-04-15-.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 1 of each calendar year; or
- (b) The company does not file documentation required by these rules showing that it has implemented that cybersecurity plan by July 1 of each calendar year.

(2) After a 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 by 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.

1220-04-15-.06 REQUIRED NOTIFICATION TO COMMISSION

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

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

1220-04-15-.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.*

* If a roll-call vote was necessary, the vote by the Agency on these rulemaking hearing rules was as follows:

Board Member	Aye	No	Abstain	Absent	Signature (if required)
Chair Herbert H. Hilliard	X				N/A
VC David F. Jones	X				N/A
Comm. Robin L. Morrison	X				N/A
Comm. Clay R. Good	X				N/A
Comm. Kenneth C. Hill				X	N/A
Comm. David Crowell	X				N/A
Comm. John Hie	X				N/A

I certify that this is an accurate and complete copy of rulemaking hearing rules, lawfully promulgated and adopted by the Tennessee Public Utility Commission on 05/08/2023, and is in compliance with the provisions of T.C.A. § 4-5-222.

I further certify the following:

Notice of Rulemaking Hearing filed with the Department of State on: 01/17/2023

Rulemaking Hearing(s) Conducted on: (add more dates). 03/20/2023

Date: 6/15/2023

Signature: Kelly Cashman Grams

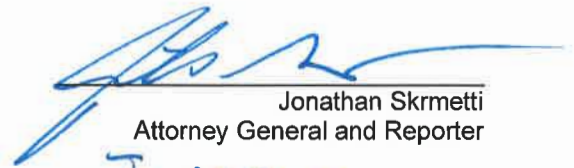
Name of Officer: Kelly Cashman Grams

Title of Officer: General Counsel

Agency/Board/Commission: Tennessee Public Utility Commission

Rule Chapter Number(s): 1220-04-15-.01 through 1220-04-15-.07

All rulemaking hearing rules provided for herein have been examined by the Attorney General and Reporter of the State of Tennessee and are approved as to legality pursuant to the provisions of the Administrative Procedures Act, Tennessee Code Annotated, Title 4, Chapter 5.


Jonathan Skrmetti
Attorney General and Reporter
June 23, 2023
Date

Department of State Use Only

RECEIVED

Jun 27 2023, 11:48 am

Secretary of State
Division of Publications

Filed with the Department of State on: 6/27/2023

Effective on: 9/25/2023


Tre Hargett
Secretary of State

Public Hearing Comments

One copy of a document that satisfies T.C.A. § 4-5-222 must accompany the filing.

The public hearing on this matter was held on March 20, 2023. Prior to the hearing, the Tennessee Public Utility Commission (Commission) issued a Notice requesting comments on the proposed rule and received comments from four parties. No party offered comments at the public hearing. All references to specific rule sections refer to the rule as submitted in January 2023, not the final rule. The substance of the comments received, and the response of the Commission are as follows:

- 1) Concerning the definition of “cybersecurity event” found in Rule 1220-04-15-.01(2), a commenter suggested that including the definition of cybersecurity event exceeds granted statutory authority. The commenter suggested that if the agency chooses to include the definition, then the agency should adopt the definition used in federal guidance for cybersecurity incident. Another commenter asserted that the rule could be improved grammatically.

Agency response: The Commission adopted the definition found in federal guidance as suggested by the commenter.

- 2) Concerning the definition of “Cybersecurity plan” as found in Rule 1220-04-15-.01(3), one commenter proposed several revisions, (1) inserting “or plans” to the definition, recognizing that a cybersecurity framework may involve more than one plan, and (2) inserting language recognizing that cybersecurity plans are designed or intended to protect the utility’s systems against unauthorized actions but are not absolute guarantees against such actions.” Another commenter suggested that the definition be expanded to include a utility’s response to a cybersecurity incident.

Agency response: The Commission adopted the changes suggested by the first commenter.

- 3) Rules 1220-04-15-.01(4) through 1220-04-15-.01(7) contain the definitions of “Information Technology,” “Operational Technology,” “Information Technology System,” and “Operational Technology System.” A commenter suggested revising the definitions of “Information Technology System” and “Operational Technology System” to match those set forth in federal guidance and deleting the definitions for “Information Technology” and “Operational Technology.”

Agency response: The Commission adopted the Commenter’s position.

- 4) With respect to Rule 1220-04-15-.02 concerning confidentiality, three commenters noted that information on company cybersecurity plans is extremely sensitive and should be handled by the agency on a confidential basis. Two parties suggested amending the rule to apply federal confidentiality requirements in addition to the state-law requirement already in the rule.

Agency response: The agency adopted the comment to add references to federal confidentiality requirements to the rule.

- 5) Rule 1220-04-15-.04(1)(a) required that the annual filing include a summary of the company’s cybersecurity program. Three commenters urged the agency to remove this rule citing the extreme sensitivity of information about cybersecurity preparedness.

Agency response: The agency removed the rule.

- 6) Rule 1220-04-15-.04(1)(d) required disclosure of plans to communicate cybersecurity incidents with the public and agency. Two commenters noted that the communications plan includes sensitive information and that too much disclosure could benefit malicious actors.

Agency response: The agency removed the rule.

- 7) Rule 1220-04-15-.04(1)(e) required the filing of an annual summary of cybersecurity incidents that result in a material loss. Two commenters noted that such information is highly sensitive. A commenter noted that the reporting requirement could create filing requirements incongruent with federal requirements. Two commenters noted that if the annual summary information filing is maintained, the filed information should be afforded the highest level of confidentiality and security.

Agency response: The agency removed the rule.

- 8) Rule 1220-04-15-.04(1)(f) required that a company disclose whether it had procured cybersecurity insurance and the current terms and limits of such coverage. Three commenters opposed the requirement concerning disclosure of the terms and limits of such coverage. One commenter noted that federal agencies recommend that companies not disclose the coverage and limits, even on a confidential basis. The two commenters added that it is well known that knowledge of coverage and limits has been used by adversaries in real-world incidents to set a ransom amount when the attackers know what their victims are willing and able to pay.

Agency response: The agency removed the requirement to disclose the terms and limits of cybersecurity insurance.

- 9) Rule 1220-04-15-.04(2) required that the documentation filed by July 1 of each year must include a sworn statement by the utility's chief executive officer, president, or another person with an equivalent role and authority. Three commenters supported the inclusion of allowing an individual with authority over the cybersecurity plan to submit the required annual documentation. One commenter suggested that it should be permitted to file an attestation in lieu of a sworn statement.

Agency response: The agency accepted the recommendation to allow individuals with authority over cybersecurity plans to make the annual filing. The agency rejected the comment to allow the filing of an attestation as it is facially inconsistent with the statutory requirement that the filing be made under oath.

- 10) Rule 1220-04-15-.06(1) required that a utility notify the agency within 48 hours of its discovery of a cybersecurity incident. One commenter supported the notification of consumers if the cybersecurity incident involved customer data or reliability of service. Three commenters noted that the notification requirement is outside the scope of the enabling legislation. The same three commenters noted that disclosure of cybersecurity incidents requires substantial investigation, and that law enforcement may require that information concerning the incident remain confidential (for a time) from the public and others, including regulators. Although the three commenters asserted that the notification requirement is outside the scope of the enabling law, they further proposed that the notification requirement be harmonized with federal reporting obligations. All four commenters noted that many industry groups and existing federal requirements require notification with a 72-hour time frame.

Agency response: The agency adopted the suggested 72-hour notification time frame and specifically acknowledged that notification may be prohibited by law enforcement. The agency did not adopt the suggestion to require notification to consumers for data breaches. The agency noted that T.C.A. § 47-18-2107 governs customer notification after a data breach.

- 11) Rule 1220-04-15-.06(2) required that within 30 days of the discovery of a cybersecurity incident, the utility shall be available and prepared to brief the agency on the cybersecurity incident. One commenter noted that there was a possibility of disclosing highly sensitive information during a briefing.

Agency response: The agency removed the rule.

Regulatory Flexibility Addendum

Pursuant to T.C.A. §§ 4-5-401 through 4-5-404, prior to initiating the rule making process, all agencies shall conduct a review of whether a proposed rule or rule affects small business.

The proposed rule impacts 28 investor-owned wastewater utilities under the jurisdiction of the Commission. The Commission believes that, currently, 21 of these utilities potentially impacted by this rule are small businesses. The rule will impact all Commission-regulated entities that become certificated natural gas, electric, water, and wastewater utilities.

The proposed rule is not anticipated to significantly increase reporting, recordkeeping, or other administrative costs relative to existing rules. The rule sets the contents of an annual filing as statutorily mandated.

The proposed rule does not duplicate or conflict with other federal, state, and local governmental rules. Cybersecurity regulation is nascent and rapidly evolving at the federal level. Generally, applicable federal regulation depends on the type of service provided by a utility. For the water and wastewater industries, the agency is not aware of a cybersecurity regulatory requirement like Tenn. Code Ann. § 65-4-127 yet created at any other governmental level.

For the natural gas industry, the U.S. Department of Homeland Security, Transportation Security Administration (DHS-TSA), in Security Directive Pipeline-2021-02C requires that the cybersecurity plan itself be transmitted to DHS-TSA annually, rather than a statement that the company has implemented a plan. Members of the electric industry did not supply comments on these rules. The agency does not believe that any company subject to these rules in the electric industry is a small business. The agency is not aware of any federal rule that conflicts with this rule.

Exemption of small businesses from the rule is not in the public interest because the requirements contained in the rule are statutorily mandated. Moreover, these requirements are necessary to assure state government officials and utility customers that appropriate prevention of and response to cybersecurity incidents has been taken to secure utility operations.

Impact on Local Governments

Pursuant to T.C.A. §§ 4-5-220 and 4-5-228, "On any rule and regulation proposed to be promulgated, the proposing agency shall state in a simple declarative sentence, without additional comments on the merits or the policy of the rule or regulation, whether the rule or regulation may have a projected financial impact on local governments. The statement shall describe the financial impact in terms of increase in expenditures or decrease in revenues."

This rule has no financial impact on local government.

Additional Information Required by Joint Government Operations Committee

All agencies, upon filing a rule, must also submit the following pursuant to T.C.A. § 4-5-226(i)(1).

- (A) A brief summary of the rule and a description of all relevant changes in previous regulations effectuated by such rule;

On June 1, 2022, Public Chapter 1111 related to utility cybersecurity plans was signed into law. The portions of the law delegating regulatory authority to the Commission are codified in Tenn. Code Ann. § 65-4-127 and require that utilities develop, implement, and maintain cybersecurity plans. The rule provides certain minimum reporting requirements, how such information will be handled for regulatory purposes, and the consequences of non-compliance.

- (B) A citation to and brief description of any federal law or regulation or any state law or regulation mandating promulgation of such rule or establishing guidelines relevant thereto;

Tenn. Code Ann. § 65-4-127 (2022)

- (C) Identification of persons, organizations, corporations or governmental entities most directly affected by this rule, and whether those persons, organizations, corporations or governmental entities urge adoption or rejection of this rule;

All Commission regulated public utilities, as defined in Tenn. Code Ann. § 65-4-101(6), are directly affected by this rule. None of TPUC regulated utilities have stated or urged in any way that the rule should be rejected. All public utilities have had opportunity to comment and those that have chosen to comment have stated agreement and satisfaction with the rule. The Consumer Advocate Division within the Financial Division of the Tennessee Attorney General, often a party appearing in proceedings before the Commission, has also commented and stated its overall satisfaction.

- (D) Identification of any opinions of the attorney general and reporter or any judicial ruling that directly relates to the rule or the necessity to promulgate the rule;

None.

- (E) An estimate of the probable increase or decrease in state and local government revenues and expenditures, if any, resulting from the promulgation of this rule, and assumptions and reasoning upon which the estimate is based. An agency shall not state that the fiscal impact is minimal if the fiscal impact is more than two percent (2%) of the agency's annual budget or five hundred thousand dollars (\$500,000), whichever is less;

Not applicable – no impact.

- (F) Identification of the appropriate agency representative or representatives, possessing substantial knowledge and understanding of the rule;

Kelly Cashman-Grams, Tim Schwarz, and Jerry Kettles

- (G) Identification of the appropriate agency representative or representatives who will explain the rule at a scheduled meeting of the committees;

Kelly Cashman-Grams and Tim Schwarz

- (H) Office address, telephone number, and email address of the agency representative or representatives who will explain the rule at a scheduled meeting of the committees; and

502 Deaderick Street, 4th Floor, Nashville TN 37243

Kelly Cashman-Grams, (615) 770-6856, Kelly.Grams@tn.gov

Tim Schwarz, (615) 770-6881, Tim.Schwarz@tn.gov

- (I) Any additional information relevant to the rule proposed for continuation that the committee requests.

None.