BEFORE THE TENNESSEE PUBLIC UTILITY COMMISSION
NASHVILLE, TENNESSEE

March 14, 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**

CHATTANOOGA GAS COMPANY'S COMMENTS

Chattanooga Gas Company ("CGC" or "Company) hereby submits its Comments in response to the Notice of Open Docket for Filing Comments, issued January 20, 2023 ("Notice"). Pursuant to the Commission's Notice seeking comments on the proposed rule in advance of the March 20, 2023, public hearing, CGC provides the following information:

I. Introduction and Background

1. CGC is incorporated under the laws of the State of Tennessee and is engaged in the business of transporting, distributing, and selling natural gas in the greater Chattanooga and Cleveland, Tennessee areas within Hamilton and Bradley Counties. CGC is a public utility pursuant to the laws of the State of Tennessee, and its public utility operations, including its rates, terms, and conditions of service, are subject to the jurisdiction of this Commission. CGC's principal office and place of business is located at 2207 Olan Mills Drive, Chattanooga, Tennessee 37421.

2. CGC requests that any parties filing comments or other pleadings in this docket

kindly provide a copy to the following representatives on behalf of CGC:

J. W. Luna, Esq
Butler Snow LLP
150 3rd Avenue South, Suite 1600
Nashville, TN 37201
Telephone: (615) 651-6749
JW.Luna@butlersnow.com

Floyd R. Self, Esq.
Berger Singerman, LLP
313 North Monroe Street, Suite 301
Tallahassee, FL 32301
Telephone: (850) 521-6727
Email: fself@bergersingerman.com

Kasey Chow, Esq.
Senior Counsel, Regulatory
Southern Company Gas
Ten Peachtree Place, NW
Atlanta, GA 30309
Telephone: (404) 584-3676
Email: kchow@southernco.com

Jason Willard
Director, External Affairs
Chattanooga Gas Company
2207 Olan Mills Drive
Chattanooga, TN 37421
Telephone: (678) 938-8558
Email: jrwillar@southernco.com

3. The Company takes protecting its digital assets as an extremely important matter of the highest priority. Various federal and state laws govern how CGC and its parent and affiliated companies store and protect its electronic systems and databases, and together the Company and its related companies make a substantial investment in people, technology, processes, and procedures to help protect the integrity of its operations and shield its customers, employees, and equipment from both physical and electronic threats and attacks. The Company commends the Commission for proceeding with this rulemaking to implement the newly enacted requirements of

Tennessee law. But in moving forward with this rulemaking, CGC offers three important modifications to the draft rules to make the rule to be adopted more consistent with existing law and current industry best practices. For convenient reference, CGC shall address each specific section of the proposed rules. Also attached is a redline/track changes version of the rule reflecting CGC's proposed edits.

II. Section 1220-04-15-.01 Definitions

4. CGC has no suggested changes to the proposed Definitions section of the draft rule.

III. Section 1220-04-15-.02 Confidentiality

5. CGC agrees that all information provided to the Commission pursuant to the rule should automatically be treated as confidential and exempt from public disclosure is consistent with the intent and purpose of the statute. Confidentiality of the security processes and procedures utilized by utilities that is to be reported to the Commission is of the greatest importance. While providing any and all cybersecurity information to the Commission on even a confidential basis is very necessary, there is still some information that should not be provided to the Commission, even on a confidential basis. Thus, it is necessary to propose some further edits to other parts of this draft rule to help ensure the integrity and security of the systems and processes the Company utilizes.

IV. Section 1220-04-15-.03 Cybersecurity Plan

6. Periodic review of the Company's cybersecurity plan is a vital component to remaining vigilant to potential threats. CGC supports the proposed minimum two-year cycle as a reasonable minimum period for such a periodic review.

V. Section 1220-04-15-.04 Annual Filing Requirements

7. Section 1 of this part of the draft rule provides for an annual attestation filing with

certain proposed minimum statements. Filing an attestation is highly preferred over filing the actual plans of the utility. Cybersecurity plans are very highly confidential given the nature of the information contained within them. Filing the actual plans with the Commission, even with confidential protection, could subject those plans to being exposed which could significantly put the Company and its customers at an unnecessary risk. CGC strongly supports filing only the attestation as set forth in the draft rule, but with two substantive modifications.

8. For Section 1, CGC has no issues or concerns with paragraphs (a), (b), (c), and (e).

9. Regarding paragraph (d), as written, the draft language is acceptable, but CGC notes that this provision needs to be read in conjunction with proposed rule 1220-4-15-.06, for which CGC is proposing an edit to the draft rule to make it consistent with other industry practices. CGC believes that a relevant and timely notification to customers is vital, but that any such notification needs to be made only after the utility has had a sufficient time to assess the extent of any potential damage to the utility's systems, procedures, ability to serve, and databases and the utility can provide meaningful information to customers regarding how they may be impacted and what, if any, actions they should take.

10. As for paragraph (f), CGC has a very grave concern for making any statement that provides any information regarding cybersecurity insurance, especially term and limits of coverage, even on a confidential basis. CGC agrees that a statement indicating the utility has cybersecurity insurance is acceptable. However, our federal partners, including the Federal Bureau of Investigation and the Department of Homeland Security, recommend that companies do not disclose the coverage and limits, even on a confidential basis. It is well known that knowledge of coverage and limits has been used by adversaries in real-world incidents to set the ransom for encryption keys and data exfiltration since the attackers know what their victims are willing and

able to pay. CGC would propose to modify this paragraph to only read, "(f) A statement indicating whether the utility has procured cybersecurity insurance." and exclude the balance of this sentence. CGC considers this to be our biggest area of concern with the draft rule and our first priority for change.

11. Section 2 of this part of the rule requires "a sworn statement by the utility's chief executive officer, president or another person with an equivalent role and authority" affirming compliance with the terms of the rule. An attestation of compliance with rules such as this one is more reasonable and sufficient in lieu of a sworn statement, which should be deleted. In addition, while it is appropriate for the CEO or president to be the reporter, the industry practice, alternatively, is to for the statement to be made by the chief security officer or cybersecurity coordinator. For example, Transportation Security Administration ("TSA") and the Illinois Commerce Commission accept an email attestation from the senior cybersecurity lead for the company. The CGC considers it a best practice to follow the TSA's lead in TSA Security Directive #1 and to utilize a cybersecurity coordinator. Accordingly, CGC would propose to strike the sworn statement require and substitute as the communication "an email or other written communication" and to expand the list of authorized individuals to include the utility's chief security officer or cybersecurity coordinator who would be authorized to make the attestations required by paragraphs (a), (b), and (c).

VI. Section 1220-04-15-.05 Failure to Comply, Sanctions

14. CGC has no suggested changes to the proposed treatment for noncompliance with the draft rule.

VII. Section 1220-04-15-.06 Required Notification to Commission of Cyber Event

12. For a utility that is a part of a large multi-utility, multi-state corporation, there can

be multiple federal and state government regulations that must be complied with in the event of a cyber attack, especially when it comes to reporting requirements – particularly to whom and when. CGC believes that consistency is extremely important in reconciling these potentially conflicting reporting requirements. However, it is imperative that the utility has sufficient time to assess the situation so it can make meaningful disclosures. Utilities need time to investigate an intrusion before reporting to regulators; utilities should not be required to report an incident until after conducting an initial mitigation and response effort to a confirmed incident. Even relatively minor cyber incidents may take hundreds of personnel hours to accurately assess what happened and the potential consequences of such an attack. A utility's first reporting obligation is to applicable law enforcement agencies (FBI, TSA, DHS, etc., as appliable) as well as entities supporting securing and mitigating further damage. For regulatory agencies that do not fall within this first group, such as this Commission, 48 hours may be too soon as the utility may not yet have a clear picture of what has occurred or law enforcement may not want disclosures to immediately occur. The FERC rule recognizes that law enforcement may not want immediate disclosures to regulators. Our natural gas industry trade associations, AGA and INGA, agree that a 72-hour deadline reflects an appropriate standard for notifying regulators about material cyber incidents. In view of these considerations, CGC would propose two changes to paragraph (a): first, 48 hours should be changed to 72 hours; and, second, at the end of the sentence the following additional language should be added, "or confirmation of a cyber event, whichever is later, with reporting made to the extent permitted by law enforcement."

VIII. Section 1220-04-15-.07 Cost Recovery for Cybersecurity Investment

13. CGC has no suggested changes to the proposed cost recovery mechanism in this section of the draft rule.

IX. Concluding Comments

WHEREFORE, CGC appreciates the Commission's invitation to provide comments regarding the implementation of this important legislation. CGC looks forward to participating in the March 20, 2023, workshop and any further proceedings the Commission may conduct in this docket.

Respectfully submitted this 14th day of March, 2023.

J. W. Luna, Esq. (No. 5780)
Butler Snow LLP
150 3rd Avenue South, Suite 1600
Nashville, TN 37201
(615) 651-6749
(615) 651-6701 facsimile
JW.Luna@butlersnow.com

and

Floyd R. Self, Esq. (TBPR PHV85597; Fla. Bar No. 608025)
Berger Singerman LLP
313 North Monroe Street, Suite 301
Tallahassee, Florida 32301
Direct Telephone: (850) 521-6727
Facsimile: (850) 561-3013
Email: fself@bergersingerman.com

Attorneys for Chattanooga Gas Company

Docket 23-00001
Attachment A
CGC Recommended Edits to the Proposed TPUC Cybersecurity Rule

Edits proposed by CGC are represented as underlined text for additions with ~~strikethrough text for deletions~~.

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) 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.

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

(8) 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.

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 that the utility has prepared and implemented a cybersecurity plan. At a minimum, the attestation shall include:

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

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

(c) A statement indicating whether the utility conducts annual cybersecurity training for the utility personnel with access to any utility IT or OT 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) 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 an email or other written communication ~~a sworn statement~~ by the utility's chief executive officer, president, chief security officer, cybersecurity coordinator, or another person with an equivalent role and authority. Such statement shall, at a minimum, 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

(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~~72 hours of the utility's discovery of the cybersecurity event or confirmation of a cyber event, whichever is later, with reporting made to the extent permitted by law enforcement.

(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.

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.