

Control Number: 49819



Item Number: 12

Addendum StartPage: 0

RECEIVED

RULEMAKING RELATING TO §  
CYBERSECURITY MONITOR §  
§

2020 JAN 27 PM 2:47  
BEFORE THE PUBLIC UTILITY COMMISSION  
OF TEXAS FILING CLERK

**ONCOR ELECTRIC DELIVERY COMPANY LLC'S AND TEXAS-NEW MEXICO  
POWER COMPANY'S INITIAL COMMENTS**

**TO THE HONORABLE PUBLIC UTILITY COMMISSION OF TEXAS:**

COMES NOW Oncor Electric Delivery Company LLC (“Oncor”) and Texas-New Mexico Power Company (“TNMP”), and timely file these initial comments on the new rule proposed in this Project, 16 Tex. Admin. Code § 25.367 (“TAC”), relating to the cybersecurity monitor (“CSM”). Oncor and TNMP appreciate the work of the Public Utility Commission of Texas (“Commission”) and Commission staff in leading the efforts in this matter, and both remain committed to working in a collaborative manner to formulate rules that will best serve the State of Texas. There are several portions of the proposed rule that Oncor and TNMP support, such as the process for selecting the CSM, the majority of the qualifications for the CSM, certain responsibilities of the CSM, the ethics standards governing the CSM, and the funding of the CSM (among other provisions). With respect to the portions of the proposed rule that Oncor and TNMP propose to revise, Oncor and TNMP respectfully show the following:

**I. INTRODUCTION**

As the Commission knows, electric transmission and distribution providers within the Electric Reliability Council of Texas, Inc. (“ERCOT”) region, such as Oncor and TNMP, are not only subject to Commission oversight and ERCOT protocols, but also subject to significant oversight from the North American Electric Reliability Corporation (“NERC”) and the Texas Reliability Entity, Inc. (“Texas RE”)<sup>1</sup> for the purpose of maintaining the reliability and security of the bulk power system. As part of this oversight, Oncor and TNMP are subject to stringent NERC reliability standards, including Critical Infrastructure

---

<sup>1</sup> Texas RE is the “Regional Entity” for the area of Texas served by ERCOT. Through a delegation agreement with NERC, which is approved by the Federal Energy Regulatory Commission, Texas RE is authorized to develop, monitor, assess, and enforce compliance with NERC reliability standards, develop regional standards, and assess and periodically report on the reliability and adequacy of the bulk power system. In addition, Texas RE serves as the Commission’s “Reliability Monitor” for the ERCOT region.

12 1

Protection (“CIP”) standards, and must submit to periodic compliance audits to assess compliance with the CIP and other reliability standards.

Prior to the introduction of the legislation proposing the creation of the CSM role, the Commission’s 2019 Scope of Competition Report (“Scope Report”) to the 86<sup>th</sup> Legislature noted that with respect to cybersecurity, the Commission “can bring value in a facilitation role.” The Scope Report went on to recommend that the Legislature “establish a collaborative cybersecurity outreach program that would bring additional resources to bear, without impeding work already being done by utilities. This program would include regular meetings with utilities to identify best practices and emerging threats, coordination of workforce training and security exercises, and related research.”<sup>2</sup>

Throughout the legislative process in which the enabling statutes behind the proposed rule were signed into law (*i.e.*, PURA §§ 36.213 and 39.1516, enacted as part of Senate Bill 936; and PURA §§ 31.051-.052 and amendments to PURA § 39.151, enacted and adopted as part of Senate Bill 64), the Legislature made clear that these statutes were intended to provide for an entity that would coordinate best efforts among utilities and conduct outreach to educate and inform utilities and the Commission about cybersecurity preparedness and best practices. For example, during the March 31, 2019 meeting of the Senate Committee on Business and Commerce, Senator Hancock laid out SB 936, describing it as follows:

“...the cybermonitor program is not intended to be the traditional regulatory compliance program ... [it is] intended to provide outreach to the Texas electric utilities to evaluate universal corporate principles and programs for infrastructure protection and to assist in identifying areas for improvement. The bill does not create new enforcement authority but instead creates a role that will allow the cybersecurity monitor to coordinate ongoing efforts across all utilities in ERCOT.”<sup>3</sup>

Additionally, in the May 31, 2019 Senate Research Center Bill Analysis for the enrolled version of SB 936, the Author’s/Sponsor’s Statement of Intent states that “[t]he cybermonitor program is not intended to be a traditional compliance standard, but rather outreach to Texas electric utilities to evaluate corporate practices and programs for infrastructure protection and assist in identifying

---

<sup>2</sup> 2019 Report on the Scope of Competition in Electric Markets in Texas, Project No. 48017, Final Version at 26-27 (Jan. 14, 2019).

<sup>3</sup> Committee video available here (see hours 1:42-1:45 for discussion of SB 936): [https://tlcsenate.granicus.com/MediaPlayer.php?view\\_id=45&clip\\_id=13987](https://tlcsenate.granicus.com/MediaPlayer.php?view_id=45&clip_id=13987).

vulnerabilities and areas for improvement.”<sup>4</sup> The language of the enabling statutes clearly reflects this specific role intended for the CSM as a facilitator, not a regulator. The Legislature never suggested there was any intention to create a new investigatory entity with oversight authority over monitored utilities.

The CSM’s role is in contrast to other grants of authority made by the Legislature such as those made to the Commission itself, the independent market monitor (“IMM”), and the reliability monitor. For example, the Commission has been granted broad authority to regulate and supervise the business of each utility<sup>5</sup> and has specifically been granted the authority to enforce provisions of PURA.<sup>6</sup> The Legislature was clear that the Commission has the authority to levy administrative penalties, disgorge profits, and seek to enjoin non-compliance.<sup>7</sup> As to the IMM, the Legislature specifically granted this entity the authority to, “...detect and prevent market manipulation strategies and recommend measures to enhance the efficiency of the wholesale market.”<sup>8</sup> As to the Reliability Monitor, the Legislature authorized the Commission to delegate to this entity responsibilities for establishing or enforcing rules relating to the reliability of the regional electrical network and accounting for the production and delivery of electricity among generators and other market participants, subject to Commission oversight and review.<sup>9</sup> No authority to monitor utilities, enforce PURA or Commission rules, or regulate utilities in any way was granted to the CSM.

Therefore, the Commission should delete from the rule all provisions that could be construed to vest the CSM with authority to require monitored utilities to submit to assessments or respond to information requests, as these provisions improperly expand the authority of the CSM beyond what is provided under the enabling statutes. Likewise, the Legislature made clear that information to be submitted by monitored utilities to the CSM is to be done on a voluntary basis.<sup>10</sup> In fact, the only difference between the introduced version

---

<sup>4</sup> Senate Research Center Bill Analysis for the enrolled version of SB 936 available here: <https://capitol.texas.gov/tlodocs/86R/analysis/pdf/SB00936F.pdf#navpanes=0>.

<sup>5</sup> See PURA § 14.001.

<sup>6</sup> See PURA §§ 15.021-.033.

<sup>7</sup> See *id.*

<sup>8</sup> PURA § 39.1515(a); see also 16 TAC § 25.365 (2019).

<sup>9</sup> PURA § 39.151(d); see also 16 TAC § 25.503(k).

<sup>10</sup> See PURA § 39.1516(b)(3).

of SB 936 and the enrolled version is the insertion of “voluntarily disclosed” in PURA § 39.1516(b)(3) in the enrolled version, signaling the Legislature’s desire to make expressly clear that the disclosure of information to the CSM is not mandatory for monitored utilities. Thus, the Commission should delete all provisions within the rule that could be construed to suggest that monitored utilities must disclose information to the CSM. As discussed in Oncor’s and TNMP’s comments below, these modifications along with additional language designed to enhance the confidential treatment of data that is provided by utilities to the CSM will contribute to a more robust program applicable to these very important issues.

## II. GENERAL COMMENTS

Before addressing certain specific provisions of the proposed rule, Oncor and TNMP provide the following general comments for the Commission’s consideration. For the convenience of the Commission, Oncor’s and TNMP’s proposed changes to the rule are shown in redline format in Attachment A and are discussed in greater detail herein.

First, Oncor and TNMP suggest that if the proposed rule is adopted, then the Commission should include a statement that the rule does not conflict with, replace or negate the applicability of any other applicable law or regulation. For example, the federal Cybersecurity Information Sharing Act of 2015 incentivizes companies to engage in the voluntary exchange of cybersecurity information with state and federal agencies by protecting such information from disclosure under the Freedom of Information Act and state sunshine laws, or use by state/federal agencies in regulatory enforcement actions.<sup>11</sup> Unintentional conflict with the processes and mechanisms in that federal law, or any other applicable law, should not be created by promulgating a regulation that is beyond the scope of the Legislature’s intent.

Further, the strawman rule expressly states that the CSM “has no enforcement authority.”<sup>12</sup> This is a very important feature of SB 936 and Oncor and TNMP applaud the inclusion of this concept in the proposed rule. This is consistent with the Commission’s rules that specifically state that the IMM has no enforcement authority.<sup>13</sup> Any suggestion of such authority could create a chilling effect under the rule, whereby monitored utilities are

---

<sup>11</sup> See 6 U.S.C. §§ 1501–10.

<sup>12</sup> Proposal for Publication at 9, subsection (g)(1).

<sup>13</sup> See 16 TAC § 25.365(e)(1).

discouraged from providing cybersecurity information to the CSM for fear that such information could potentially lead to enforcement actions that would be detrimental to utilities.

### **III. SPECIFIC COMMENTS**

In addition to the general comments set forth above, Oncor and TNMP provide the following comments concerning specific provisions of the proposed rule. As with Oncor's and TNMP's general comments, these specific comments are reflected in redline format in Attachment A.

#### **A. Subsection (e) – Qualifications of CSM.**

Subsection (e) of the rule sets forth the qualifications of the CSM, but in doing so, subsection (e)(2) also lists the “cybersecurity monitoring functions” that the CSM must be able to perform. One such function includes “conducting vulnerability assessments.”<sup>14</sup> This current wording suggests that the CSM could have the authority to probe monitored utilities for information in order to conduct its own audits or assessments of the monitored utility's cybersecurity system's vulnerabilities. This was not the intent of the Legislature. The Legislature did not authorize this in the enabling statutes and, instead, only contemplated self-assessments that may be voluntarily performed by monitored utilities. Therefore, subsection (e)(2)(C) is overly broad and should be deleted or, at a minimum, reworded in a manner that tracks the language of PURA § 39.1516(b)(3), such as: “reviewing self-assessments voluntarily disclosed by monitored utilities of cybersecurity efforts.” Without this deletion or change, subsection (e)(2)(C), when read in conjunction with other parts of the rule, could create ambiguity as to whether the CSM has authority to require monitored utilities to submit to vulnerability assessments the CSM wishes to conduct. The CSM does not have any such authority.

#### **B. Subsection (g) – Authority of the CSM.**

Subsection (g)(1) of the rule gives the CSM broad authority to engage in “monitoring, analysis, reporting, and related activities.” As discussed above in the general comments, the enabling legislation does not vest the CSM with any ability to impose reporting or documentation requirements on monitored utilities, or any ability to oversee, investigate, or

---

<sup>14</sup> Proposal for Publication at 7, subsection (e)(2)(C).

audit monitored utilities. Instead, the enabling legislation creates a new role in which the selected entity is to develop and coordinate an outreach program through which it will communicate information *to utilities*, rather than requiring monitored utilities to report information *to the CSM*. While PURA § 39.1516(b)(3) contemplates voluntary self-assessments, nowhere does the legislation empower the CSM to require monitored utilities to conduct and report on self-assessments or to submit to CSM-initiated assessments or monitoring. Oncor and TNMP have every intention of collaborating with the CSM and participating in the various programs, but the Commission should be reticent to enact a rule that gives any suggestion that monitored utilities are under any obligation to release sensitive information to the CSM.

Oncor and TNMP manage their sensitive cyber information with due care and diligence and are aware of the magnitude of potential harm that could occur if the information is disclosed to the CSM and the CSM system is subsequently breached. In fact, and for example, because of the risk of disclosure when Oncor's sensitive cyber information is provided to an entity other than Oncor, this information never leaves Oncor's control. Given that the CSM will be a third-party entity without a proven track record of securely maintaining critical infrastructure and cybersecurity information, there is even more of a risk that its system could be breached. This risk further justifies a significant change to subsection (g). For these reasons, subsection (g)(1) should be reworded as follows: "[t]he CSM has the authority to conduct cybersecurity-related outreach meetings, reviews of voluntarily disclosed self-assessments, research and development of best practices, and reporting, but has no enforcement authority."<sup>15</sup>

Next, subsection (g)(2) of the rule states that "[t]he CSM has the authority to request information from a monitored utility about activities that may be potential cybersecurity threats." Subsection (g)(3) then states that "[t]he CSM is authorized to require that each monitored utility designate one or more points of contact who can answer questions the CSM may have regarding a monitored utility's cyber and physical security activities." There is no guidance in the rule, however, as to whether a monitored utility is required to provide information responsive to requests made by the CSM under (g)(2), or whether the designated point of contact is required to answer questions received from the CSM under (g)(3). The

---

<sup>15</sup> See PURA § 39.1516(b)(1)-(5), (f).

answer to both questions is “no,” given that the Legislature has not imposed any obligation on monitored utilities to provide any information to the CSM, whether requested by the CSM or not. However, subsections (g)(2) and (g)(3) of the rule could create ambiguity and uncertainty as to the obligations of a monitored utility. Therefore, subsections (g)(2) and (g)(3) should be deleted. In the event that the Commission declines to strike subsections (g)(2) and (g)(3), then Oncor and TNMP urge the Commission to include additional language in subsection (g) or elsewhere in the rule to clarify that a monitored utility’s decision to submit information responsive to a request from the CSM is purely voluntary, rather than mandatory, and that the CSM is prohibited from pressuring a monitored utility into providing information that the utility prefers to protect from disclosure.

**C. Subsection (i) – Confidentiality Standards; and subsection (l) – ERCOT’s responsibilities and support role.**

As currently worded, subsection (i) states:

The CSM and commission staff must protect confidential information and data in accordance with the confidentiality standards established in PURA, the ERCOT protocols, commission rules, and other applicable laws. The requirements related to the level of protection to be afforded information protected by these laws and rules are incorporated in this section.<sup>16</sup>

Oncor and TNMP suggest that this language should be enhanced to also include the confidentiality language included in subsection (l)(3) of the rule,<sup>17</sup> in order to expressly state that any cybersecurity information obtained or compiled by the CSM or provided by the CSM to the Commission must be treated as confidential information and shall not be subject to public disclosure under Chapter 552 of the Government Code (or otherwise). This addition

---

<sup>16</sup> Proposal for Publication at 11.

<sup>17</sup> See Proposal for Publication at 12, subsection (l)(3), which states: “[i]nformation submitted in the report under paragraph (2) of this subsection is confidential and not subject to disclosure under chapter 552, Government Code.”



would ensure that the confidentiality obligations under subsection (i) comport with PURA §§ 39.1516(g)<sup>18</sup> and 39.1516(h).<sup>19</sup>

Likewise, Oncor and TNMP suggest that the confidentiality language in subsection (l)(3) should be enhanced to also include the requirement to protect data “in accordance with the confidentiality standards established in PURA, the ERCOT protocols, commission rules, and other applicable laws,” as currently included in subsection (i), so that both confidentiality provisions provide adequate protection of critical cybersecurity data.

Additionally, Oncor and TNMP urge the Commission to include language in the subsection (i) confidentiality provision that expressly limits the entities or individuals that may receive information compiled by or voluntarily disclosed to the CSM, and requires the CSM and Commission to source-anonymize the information so that it cannot be traced to the entity that disclosed it. Because this information should be exempt from disclosure to the general public, and because only a narrow category of entities would have a legitimate need for obtaining such information, the rule should expressly list the appropriate recipients who may request access to such information, such as the Commission and ERCOT. Other third-party entities and individuals should not be permitted to obtain access to the information unless they have been vetted pursuant to appropriate standards and the information has been source-anonymized prior to disclosure to such entities.

**D. Subsection (m)(1) – Participation in the cybersecurity monitor program.**

Subsection (m)(1) states that utilities and other specified entities subject to the rule “must participate” in the cybersecurity monitor program. As explained above, it is clear from the enabling legislation that monitored utilities are not required to (but may voluntarily choose to) submit any particular information to the CSM that may be requested by the CSM, disclose information that may be pertinent to the monitored utility’s cybersecurity efforts, or submit to assessments conducted by the CSM. For these reasons, subsection (m)(1) should be changed to reflect the voluntary aspect of the legislation. Oncor and TNMP also suggest that a conforming change be made to subsection (a), such that “participation in the cybersecurity

---

<sup>18</sup> PURA § 39.1516(g) states in relevant part: “[c]ommission staff may not disclose information obtained under this section in an open meeting or through a response to a public information request.”


<sup>19</sup> PURA § 39.1516(h) states in relevant part: “[i]nformation written, produced, collected, assembled, or maintained under Subsection (b), (c), or (g) is confidential and not subject to disclosure under Chapter 552, Government Code.”

monitor program” be revised to read “voluntary participation in the cybersecurity monitor program.”

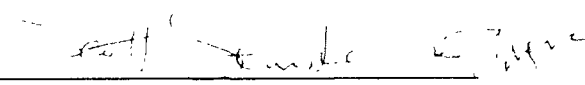
#### IV. CONCLUSION

Oncor and TNMP appreciate the opportunity to comment on the strawman rule and respectfully request the Commission’s consideration of the comments set forth in this pleading.

Respectfully submitted,

  
By: \_\_\_\_\_  
Myles F. Reynolds  
State Bar No. 24033002  
Lauren Freeland  
State Bar No. 24083023  
Hunton Andrews Kurth LLP  
1445 Ross Avenue, Suite 3700  
Dallas, Texas 75202  
Phone: (214) 979-3069  
Facsimile: (214) 880-0011  
mreynolds@huntonak.com


**ATTORNEYS FOR ONCOR ELECTRIC  
DELIVERY COMPANY LLC**

  
By: \_\_\_\_\_  
Scott Seamster  
State Bar No. 00784939  
Corporate Counsel  
Texas-New Mexico Power Company  
577 N. Garden Ridge Blvd.  
Lewisville, Texas 75067  
Phone: (214) 224-4143  
Facsimile: (214) 224-4156  
scott.seamster@pnmresources.com

**ATTORNEY FOR TEXAS-NEW MEXICO  
POWER COMPANY**

**CERTIFICATE OF SERVICE**

I hereby certify that a true and correct copy of the foregoing has been e-mailed, hand delivered, or sent via overnight delivery or first-class United States mail, postage prepaid, to the Staff of the Public Utility Commission of Texas on this ~~the~~ 27th day of January, 2020.

  
\_\_\_\_\_

## ATTACHMENT A

### 1 § 25.367. Cybersecurity Monitor.

2 (a) **Purpose.** This section establishes requirements for the commission's cybersecurity  
3 coordination program, the cybersecurity monitor program, the cybersecurity monitor, and  
4 voluntary participation in the cybersecurity monitor program; and establishes the methods  
5 to fund the cybersecurity monitor. This section is not intended to replace or negate any  
6 other applicable law or regulation.

7  
8 (b) **Applicability.** This section is applicable to all electric utilities, including transmission  
9 and distribution utilities; corporations described in Public Utility Regulatory Act (PURA)  
10 §32.053; municipally owned utilities; electric cooperatives; and the Electric Reliability  
11 Council of Texas (ERCOT).

12  
13 (c) **Definitions.** The following words and terms when used in this section have the following  
14 meanings, unless the context indicates otherwise:

15 (1) **Cybersecurity monitor (CSM)** -- The entity selected by the commission to serve  
16 as the commission's cybersecurity monitor and its staff.

17 (2) **Cybersecurity coordination program** -- The program established by the  
18 commission to monitor the cybersecurity efforts of all electric utilities,  
19 municipally owned utilities, and electric cooperatives in the state of Texas.

20 (3) **Cybersecurity monitor program** -- The comprehensive outreach program for  
21 monitored utilities managed by the CSM.

22 (4) **Monitored utility** -- A transmission and distribution utility; a corporation  
23 described in PURA §32.053; a municipally owned utility or electric cooperative

1 that owns or operates equipment or facilities in the ERCOT power region to  
2 transmit electricity at 60 or more kilovolts; or an electric utility, municipally  
3 owned utility, or electric cooperative that operates solely outside the ERCOT  
4 power region that has elected to participate in the cybersecurity monitor program.

5  
6 (d) **Selection of the CSM.** The commission and ERCOT will contract with an entity  
7 selected by the commission to act as the commission's CSM. The CSM must be  
8 independent from ERCOT and is not subject to the supervision of ERCOT. The CSM  
9 must operate under the supervision and oversight of the commission.

10  
11 (e) **Qualifications of CSM.**

12 (1) The CSM must have the qualifications necessary to perform the duties and  
13 responsibilities under subsection (f) of this section.

14 (2) The CSM must collectively possess a set of technical skills necessary to perform  
15 cybersecurity monitoring functions that include:

16 (A) developing, reviewing, and implementing cybersecurity risk management  
17 programs, cybersecurity policies, cybersecurity strategies, and similar  
18 governance documents; and

19 (B) working knowledge of North American Electric Reliability Corporation  
20 Critical Infrastructure Protection (NERC CIP) standards and  
21 implementation of those standards; ~~and~~

22 ~~(C) conducting vulnerability assessments.~~



- 1 (iii) vendor remote access.
- 2 (2) **Cybersecurity Monitor Program.** The cybersecurity monitor program is  
3 available to all monitored utilities. The cybersecurity monitor program must  
4 include the functions of the cybersecurity coordination program listed in  
5 paragraph (1) of this subsection and the following functions:
- 6 (A) holding regular meetings with monitored utilities to discuss emerging  
7 threats, best business practices, and training opportunities;
- 8 (B) reviewing self-assessments of cybersecurity efforts voluntarily disclosed  
9 by monitored utilities; and
- 10 (C) reporting to the commission on monitored utility cybersecurity  
11 preparedness.

12

13 (g) **Authority of the CSM.**

- 14 ~~(1) — The CSM has the authority to conduct cybersecurity-related outreach meetings,~~  
15 ~~reviews of voluntarily disclosed self-assessments, research and development of~~  
16 ~~best practices, and reporting, monitoring, analysis, reporting, and related activities~~  
17 ~~but has no enforcement authority.~~
- 18 ~~(2) — The CSM has the authority to request information from a monitored utility about~~  
19 ~~activities that may be potential cybersecurity threats.~~
- 20 ~~(3) — The CSM is authorized to require that each monitored utility designate one or~~  
21 ~~more points of contact who can answer questions the CSM may have regarding a~~  
22 ~~monitored utility's cyber and physical security activities.~~

23

1 (h) **Ethics standards governing the CSM.**

2 (1) During the period of a person's service with the CSM, the person must not:

3 (A) have a specific interest in the commission's regulation and must not have a  
4 direct financial interest in the provision of electric service in the state of  
5 Texas; or have a current contract to perform services for any entity as  
6 described by PURA §31.051 or a corporation described by PURA §32.053.

7 (B) serve as an officer, director, partner, owner, employee, attorney, or  
8 consultant for ERCOT or any entity as described by PURA §31.051 or a  
9 corporation described by PURA §32.053;

10 (C) directly or indirectly own or control securities in any entity, an affiliate of  
11 any entity, or direct competitor of any entity as described by PURA  
12 §31.051 or a corporation described by PURA §32.053, except that it is not  
13 a violation of this rule if the person indirectly owns an interest in a  
14 retirement system, institution or fund that in the normal course of business  
15 invests in diverse securities independently of the control of the person; or

16 (D) accept a gift, gratuity, or entertainment from ERCOT, any entity, an  
17 affiliate of any entity, or an employee or agent of any entity as described  
18 by PURA §31.051 or a corporation described by PURA §32.053.

19 (2) The CSM director or a CSM staff member must not directly or indirectly solicit,  
20 request from, suggest, or recommend to any entity, an affiliate of any entity, or an  
21 employee or agent of any entity as described by PURA §31.051 or a corporation  
22 described by PURA §32.053, the employment of a person by any entity as



1 described by PURA §31.051 or a corporation described by PURA §32.053 or an  
2 affiliate.

3 (3) The commission may impose post-employment restrictions for the CSM and its  
4 staff.

5  
6 (i) **Confidentiality standards.**

7 (1) The CSM and commission staff must protect confidential information and data in  
8 accordance with the confidentiality standards established in PURA, the ERCOT  
9 protocols, commission rules, and other applicable laws. The requirements related  
10 to the level of protection to be afforded information protected by these laws and  
11 rules are incorporated in this section. Cybersecurity information obtained or  
12 compiled by the CSM or provided by the CSM to commission staff must be  
13 treated as confidential information and shall not be subject to public disclosure,  
14 either under chapter 552 of the Government Code or otherwise.

15 (2) Cybersecurity information obtained or compiled by the CSM may be provided  
16 only to (i) commission staff, and (ii) to the extent requested and reasonably  
17 necessary, ERCOT.

18 (3) The CSM shall not provide data obtained from a monitored utility pursuant to  
19 (i)(2) unless the data is provided such that the identity of the monitored utility  
20 remains anonymous.

21

1 (j) **Reporting requirement.** All reports prepared by the CSM must reflect the CSM's  
2 independent analysis, findings, and expertise. The CSM must prepare and submit to the  
3 commission:

4 (1) monthly, quarterly, and annual reports; and

5 (2) periodic or special reports on cybersecurity issues or specific events as directed by  
6 the commission or commission staff.

7

8 (k) **Communication between the CSM and the commission.**

9 (1) The personnel of the CSM may communicate with the commission and  
10 commission staff on any matter without restriction consistent with confidentiality  
11 requirements.

12 (2) The CSM must:

13 (A) immediately report directly to the commission and commission staff any  
14 potential cybersecurity concerns;

15 (B) regularly communicate with the commission and commission staff, and  
16 keep the commission and commission staff apprised of its activities,  
17 findings, and observations;

18 (C) coordinate with the commission and commission staff to identify  
19 priorities; and

20 (DE) coordinate with the commission and commission staff to assess the  
21 resources and methods for cybersecurity monitoring, including consulting  
22 needs.

23

1 (l) **ERCOT's responsibilities and support role.** ERCOT must provide to the CSM any  
2 access, information, support, or cooperation that the commission determines is necessary  
3 for the CSM to perform the functions described by subsection (f) of this section.

4 (1) ERCOT must conduct an internal cybersecurity risk assessment, vulnerability  
5 testing, and employee training to the extent that ERCOT is not otherwise required  
6 to do so under applicable state and federal cybersecurity and information security  
7 laws.

8 (2) ERCOT must submit an annual report to the commission on ERCOT's  
9 compliance with applicable cybersecurity and information security laws by  
10 January 15 of each year or as otherwise determined by the commission.

11 (3) Information submitted in the report under paragraph (2) of this subsection is  
12 confidential and not subject to disclosure under chapter 552, Government Code,  
13 and must be protected in accordance with the confidentiality standards established  
14 in PURA, the ERCOT protocols, commission rules, and other applicable laws.  
15  
16

17 (m) **Participation in the cybersecurity monitor program.**

18 (1) A transmission and distribution utility, a corporation described in PURA §32.053,  
19 and a municipally owned utility or electric cooperative that owns or operates  
20 equipment or facilities in the ERCOT power region to transmit electricity at 60 or  
21 more kilovolts ~~must~~ may participate in the cybersecurity monitor program.

22 (2) An electric utility, municipally owned utility, or electric cooperative that operates  
23 solely outside the ERCOT power region may elect to participate in the

1           cybersecurity monitor program. An electric utility, municipally owned utility, or  
2           electric cooperative that operates solely outside the ERCOT power region that  
3           elects to participate in the cybersecurity monitoring program is a monitored utility.

4           (A) An electric utility, municipally owned utility, or electric cooperative that  
5           elects to participate in the cybersecurity monitor program must annually:

6           (i) file with the commission its intent to participate in the program and  
7           to contribute to the costs of the CSM's activities in the project  
8           established by commission staff for this purpose; and

9           (ii) complete and submit to ERCOT the participant agreement form  
10          available on the ERCOT website to furnish information necessary  
11          to determine and collect the monitored utility's share of the costs  
12          of the CSM's activities under subsection (n) of this section.

13          (B) The cybersecurity monitor program year is the calendar year. An electric  
14          utility, municipally owned utility, or electric cooperative that elects to  
15          participate in the cybersecurity monitor program must file its intent to  
16          participate and complete the participant agreement form under  
17          subparagraph (A) of this subsection for each calendar year that it intends to  
18          participate in the program.

19          (i) Notification of intent to participate and a completed participant  
20          agreement form may be submitted at any time during the program  
21          year, however, an electric utility, municipally owned utility, or  
22          electric cooperative that elects to participate in an upcoming  
23          program year is encouraged to complete these steps by December 1

1 prior to the program year in order to obtain the benefit of  
2 participation for the entire program year.

3 (ii) The cost of participation is determined on an annual basis and will  
4 not be prorated.

5 (iii) A monitored utility that elected to participate under subsection  
6 (m)(2) may discontinue its participation in the cybersecurity  
7 monitor program at any time but is required to pay the annual cost  
8 of participation for any calendar year in which the monitored utility  
9 submitted a notification of intent to participate.

10

11 (n) **Funding of the CSM.**

12 (1) ERCOT must use funds from the rate authorized by PURA §39.151(e) to pay for  
13 the CSM's activities.

14 (2) A monitored utility that operates solely outside of the ERCOT power region must  
15 contribute to the costs incurred for the CSM's activities.

16 (A) On an annual basis, ERCOT must calculate the non-refundable, fixed fee  
17 that a monitored utility that operates solely outside of the ERCOT power  
18 region must pay in order to participate in the cybersecurity monitor  
19 program for the upcoming calendar year.

20 (B) ERCOT must file notice of the fee in the project designated by the  
21 commission for this purpose and post notice of the fee on the ERCOT  
22 website.

- 1 (i) For the 2020 program year, ERCOT must file and post notice of
- 2 the fee to participate in the program by May 1, 2020.
- 3 (ii) Beginning with the 2021 program year, ERCOT must file and post
- 4 notice of the fee to participate in the program by October 1 of the
- 5 preceding program year.
- 6 (C) Before filing notice of the fee as required by paragraph (2)(B) of this
- 7 subsection, ERCOT must obtain approval of the fee amount and
- 8 calculation methodology from the commission's executive director.
- 9
- 10

1           This agency certifies that the proposal has been reviewed by legal counsel and found to be  
2 within the agency’s legal authority to adopt.

3

4           **ISSUED IN AUSTIN, TEXAS ON THE \_\_\_\_\_ DAY OF \_\_\_\_\_ 2019 BY THE**  
5                           **PUBLIC UTILITY COMMISSION OF TEXAS**  
6                           **ANDREA GONZALEZ**

7

8