



Control Number: 49819



Item Number: 22

Addendum StartPage: 0

**PROJECT NO. 49819**

**RULEMAKING RELATING TO  
CYBERSECURITY MONITOR**

§  
§  
§

**PUBLIC UTILITY COMMISSION**

**OF TEXAS**

**ORDER ADOPTING NEW 16 TAC §25.367  
AS APPROVED AT THE MAY 14, 2020 OPEN MEETING**

The Public Utility Commission of Texas (commission) adopts new §25.367, relating to cybersecurity monitor, with changes to the proposed text as published in the December 27, 2019 issue of the *Texas Register* (44 TexReg 8189). The rule will establish a cybersecurity coordination program to monitor cybersecurity efforts among electric utilities, electric cooperatives, and municipally owned electric utilities in the state, as required by Senate Bill (SB) 64, relating to cybersecurity for information resources, 86th Legislature, Regular Session; and will establish a cybersecurity monitor, a cybersecurity monitor program, and the method to fund the cybersecurity monitor, as required by SB 936, relating to cybersecurity monitor for certain electric utilities, 86th Legislature, Regular Session. This new section is adopted under Project No. 49819.

The commission received comments on the proposed rule from CenterPoint Energy Houston Electric, LLC (CenterPoint); the Electric Reliability Council of Texas, Inc. (ERCOT); Lower Colorado River Authority (LCRA); Office of Public Utility Counsel (OPUC); Oncor Electric Delivery Company LLC (Oncor) and Texas-New Mexico Power Company (TNMP); Southwestern Public Service Company, El Paso Electric Company, and Entergy Texas, Inc.,

(collectively the Integrated Utilities); Texas Electric Cooperatives, Inc., (TEC); and Texas Public Power Association (TPPA). There was no request for a public hearing.

*General Comments on §25.367*

CenterPoint, LCRA, OPUC, TEC, and TPPA generally supported the proposed rule, which implements SB 64 and SB 936 by establishing requirements for a cybersecurity coordination program, a cybersecurity monitor, and cybersecurity monitoring program. ERCOT supported the proposed rule with respect to the provisions applicable to ERCOT. Oncor and TNMP supported several portions of the proposed rule including the process for selection of the cybersecurity monitor, most of the qualifications for the cybersecurity monitor, certain responsibilities of the cybersecurity monitor, the ethics standards governing the cybersecurity monitor, and funding of the cybersecurity monitor.

LCRA, Oncor, TNMP, and TPPA stated that the statute did not grant authority to the cybersecurity monitor to monitor utilities, enforce the Public Utility Regulatory Act (PURA) or commission rules, or regulate utilities.

Oncor, TNMP, LCRA, and TPPA stated that the Legislature made clear that information submitted by utilities to the cybersecurity monitor is to be disclosed voluntarily. LCRA and TPPA supported establishment of a cybersecurity monitor and cybersecurity programs that focus on outreach, research, facilitating the distribution of information to utilities, and the development of best practices.

Oncor and TNMP suggested adding a statement to the proposed rule that the rule does not conflict with, replace, or negate the applicability of any other applicable law or regulation.

The Integrated Utilities requested clarification regarding the manner in which the cybersecurity coordination program and cybersecurity monitor program will coexist if all utilities do not elect to participate in the cybersecurity monitor program, why two programs are necessary, and the manner in which the programs' operations will vary. The Integrated Utilities also requested that a subsection be added to address utility cost recovery.

#### *Commission Response*

In this rule, the commission is implementing two bills, SB 64 and SB 936. SB 64 established a cybersecurity coordination program for electric cooperatives, electric utilities, municipally owned electric utilities, and transmission and distribution utilities throughout the state to provide guidance on best practices in cybersecurity and facilitate sharing of information. SB 936 established a cybersecurity monitor program for transmission and distribution utilities, a corporation described in PURA §32.053 (Lower Colorado River Authority Transmission Services Corporation), and municipally owned utilities or electric cooperatives in the ERCOT region that own or operate equipment or facilities to transmit electricity at 60 or more kilovolts. Electric utilities, municipally owned utilities, and electric cooperatives operating outside the ERCOT region may also elect to participate in the program. New §25.367 is intended to harmonize the requirements of the two bills. Any utility in Texas may participate in the cybersecurity coordination program at no cost. The cybersecurity monitor program includes the additional features set out in §25.367(f)(2) that

are available to monitored utilities. Monitored utilities in the ERCOT region will contribute to the costs of the cybersecurity monitor program through payment of the ERCOT administrative fee. Monitored utilities that operate solely outside the ERCOT region will contribute to the costs of the cybersecurity monitor program by payment of the fee established under §25.367(n)(2).

The commission responds to the other issues raised in the general comments in the commission responses to comments in the applicable subsections of the proposed rule.

*Comments on §25.367(a) (Purpose)*

This subsection describes the purpose of the rule: to establish requirements for the commission's cybersecurity coordination program, the cybersecurity monitor program, the cybersecurity monitor, and participation in the cybersecurity monitor program; and to establish the methods to fund the cybersecurity monitor.

LCRA, Oncor, and TNMP recommended adding the word "voluntary" before cybersecurity monitor program to clarify that participation in the cybersecurity monitor program is voluntary; and add the statement "This section is not intended to replace or negate any other applicable law or regulation." TPPA supported this recommendation.

*Commission Response*

The commission declines to make the requested changes in the purpose statement because they are unnecessary. The voluntary nature of participation in the cybersecurity

**coordination and cybersecurity monitor programs is made clear throughout the rule. The commission declines to add the statement about replacing or negating other applicable law or regulation, because it is unnecessary and as recommended, overly broad.**

*Comments on §25.367(e) (Qualifications of the cybersecurity monitor)*

The Integrated Utilities recommended that §25.367(e)(2) relating to qualifications of the cybersecurity monitor be rewritten to add “Those skills include:” immediately following the revised sentence “The cybersecurity monitor must collectively possess a set of technical skills necessary to perform cybersecurity monitoring functions.”

*Commission Response*

**The commission modifies §25.367(e)(2) for clarity.**

LCRA stated that the commission should ensure the qualifications of the cybersecurity monitor align with the legislatively prescribed purpose of this new entity. LCRA recommended that the word “governance” be replaced with “best practices” before “documents” in §25.367(e)(2)(A) to avoid confusion about the role of the cybersecurity monitor and its authority.

*Commission Response*

**The commission declines to insert the phrase “best practices” as proposed by LCRA and deletes the word “governance” before the word “documents” because using a modifier for the word “documents” is unnecessary and could cause confusion.**

Oncor, TNMP, and TPPA supported removal or modification of §25.367(e)(2)(C), which requires the cybersecurity monitor to have the technical skills to conduct vulnerability assessments. Oncor, TNMP, and LCRA asserted that the provision is not consistent with the intent of the Legislature. Oncor and TNMP stated that the provision 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.” Further, Oncor and TNMP asserted that if the provision is not deleted or modified, it could create ambiguity as to whether the cybersecurity monitor has authority to require monitored utilities to submit to the vulnerability assessments the cybersecurity monitor wishes to conduct. TPPA recommended that if the commission declines to revise the rule language, then the information analyzed should consist only of the monitored utility’s voluntary self-assessments, or that information used by the cybersecurity monitor to conduct vulnerability assessments be routed through monitored utility points of contact instead of directly collected by the cybersecurity monitor. LCRA recommended that the provision be deleted.

### ***Commission Response***

**The commission declines to modify §25.367(e)(2)(C). Subsection 25.367(e) describes the required qualifications for the cybersecurity monitor and does not, in itself, confer any authority. The commission agrees that the cybersecurity monitor does not have the authority to require monitored utilities to submit to vulnerability assessments or to produce documents or other information related to any such assessments. Nevertheless, the cybersecurity monitor must have the skills necessary to perform vulnerability assessments to competently provide services to utilities that request assistance in this area.**

*Comments on §25.367(f) (Responsibilities of the cybersecurity monitor)*

CenterPoint stated that the language in §25.367(f), which relates to the responsibilities of the cybersecurity monitor, appropriately lists the cybersecurity monitor's responsibilities associated with the cybersecurity programs consistent with the enabling legislation.

LCRA stated that additional clarity is needed regarding whose data and information will be gathered by the cybersecurity monitor. LCRA recommended changes to add the cybersecurity monitor's responsibility to collect information from ERCOT; to reiterate that provision of information by electric utilities is voluntary; and to remove the words "analyze," "as-needed," and the reference to the cybersecurity coordination program. LCRA stated that these changes are necessary to track the Legislature's specific grants of authority as codified in PURA §39.1516(b)(3) and (c). LCRA added that, because the Legislature did not authorize data gathering from electric utilities as part of SB 64, this provision should not reference the cybersecurity coordination program. TPPA supported LCRA's recommendation.

In an effort to leverage information already maintained by utility staff, the Integrated Utilities suggested that utility self-assessments and other information gathering be based on commonly used security control standards such as those published in the National Institute of Standards and Technology (NIST) document, NIST 800-53.



*Commission Response*

The commission modifies §25.367(f) to add ERCOT as a possible source of information and to emphasize the voluntary nature of information sharing but declines to remove the reference to the cybersecurity coordination program. The cybersecurity monitor's responsibilities span both programs covered by the new rule. The commission agrees that utility self-assessments and other information gathering should be based on commonly used standards but will not reference specific standards in the rule. The commission anticipates that the cybersecurity monitor will work with monitored utilities to ensure that appropriate security control standards are used.

*Comments on §25.367(g) (Authority of the cybersecurity monitor)*

Oncor and TNMP stated that the Legislature did not grant the cybersecurity monitor authority to monitor utilities, enforce PURA or commission rules, or regulate utilities in any way. Oncor, TNMP and LCRA stated that the legislation establishing the cybersecurity monitor did not vest the cybersecurity monitor with any ability to impose reporting or documentation requirements on monitored utilities or any ability to oversee, investigate, or audit monitored utilities. Oncor and TNMP asserted that the cybersecurity monitor's mandated role is to develop and coordinate an outreach program to communicate information to utilities, rather than requiring monitored utilities to report information to the cybersecurity monitor. Oncor, TNMP, and LCRA recommended rule language to modify §25.367(g)(1) to clarify the role of the cybersecurity monitor.

The Integrated Utilities requested that the cybersecurity monitor's monitoring authority be limited to obtaining the information furnished in North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) and other existing assessments. They argued that this limitation would ensure that they do not need to generate new processes or materials for the cybersecurity monitor. To clarify that provision of information to the cybersecurity monitor is voluntary, the Integrated Utilities suggested adding "as agreed upon by the monitored utility" after "The cybersecurity monitor has the authority to conduct monitoring, analysis, reporting, and related activities" in §25.367(g)(1). Similarly, the Integrated Utilities suggested adding "which the monitored utility, in its sole discretion may provide to the cybersecurity monitor" to §25.367(g)(2).

CenterPoint and TPPA stated that the language in §25.367(g) could be interpreted as providing authority to the cybersecurity monitor not granted by legislation. To track the legislative intent for the cybersecurity programs and to clarify the relationship between §25.367 (g) and (f), CenterPoint recommended that §25.367(g)(1) be revised to provide that the cybersecurity monitor has the authority to carry out the responsibilities under §25.367(f); §25.367(g)(2) be deleted; and the description "who can answer questions the cybersecurity monitor may have" be removed from the one or more points of contact each monitored utility is required to designate in §25.367(g)(3).

Under §25.367(g)(2), the cybersecurity monitor has the authority to request certain information from a monitored utility, and §25.367(g)(3) provides that the cybersecurity monitor is authorized to request that each monitored utility designate one or more points of contact who can answer

questions the cybersecurity monitor may have regarding a monitored utility's cyber and physical security activities. Oncor and TNMP stated that the rule is unclear as to whether a monitored utility is required to provide information responsive to the cybersecurity monitor's request under §25.367(g)(2), or whether the designated point of contact under §25.367(g)(3) is required to answer questions received from the cybersecurity monitor. LCRA agreed with Oncor and TNMP that, because the Legislature did not impose any obligation on the monitored utility to provide any information to the cybersecurity monitor, §25.367(g)(2) and (g)(3) should be deleted. In the alternative, Oncor and TNMP suggested that the commission modify the rule language to clarify that a monitored utility's decision to submit information responsive to a request from the cybersecurity monitor is purely voluntary, and that the cybersecurity monitor is prohibited from pressuring a monitored utility to provide information.

TEC stated that no single point of contact may have all the information needed to respond to the cybersecurity monitor's questions. TEC recommended that §25.367(g)(3) be revised to allow each monitored utility's points of contact to coordinate answers to questions the cybersecurity monitor may have.

### ***Commission Response***

**The commission does not intend to confer authority on the cybersecurity monitor that is not granted by statute and modifies §25.367(g) to clarify the role of the cybersecurity monitor. The modifications clarify the voluntary nature of interactions between monitored utilities and the cybersecurity monitor. Because monitored utilities are not required to provide any documents to the cybersecurity monitor, it is not necessary to limit the types of**

documents that may be requested by, or provided to, the cybersecurity monitor. The commission removes statements about the cybersecurity monitor's enforcement authority because it is unnecessary to include such statements in the rule. Further, the obligation to designate one or more contact persons is clarified to be a requirement imposed by the commission, rather than the cybersecurity monitor. Accordingly, this provision has been relocated to §25.367(m). The commission declines to modify the requirement as recommended by TEC because coordination of responses to information requests is inherent in the role of a contact person.

TEC and the Integrated Utilities stated that physical security is beyond the scope of the cybersecurity legislation and recommended that the reference to it be removed from §25.367(g)(3).

#### *Commission Response*

The commission does not agree that physical security is beyond of the scope of the cybersecurity monitor program and declines to remove the reference to physical security. Physical security is a component of cybersecurity and is part of the "Defense In Depth" strategy widely used within the cybersecurity industry and seen as a best business practice. The commission recognizes that there are aspects of physical security that are not related to cybersecurity and does not intend for the cybersecurity monitor program to extend to such areas.

*Comments on §25.367(i) (Confidentiality standards)*

CenterPoint strongly supported the proposed rule language that protects the confidentiality of information related to the cybersecurity coordination and cybersecurity monitor programs. CenterPoint stated that §25.367(i) appropriately requires the cybersecurity monitor and commission staff to protect confidential information in accordance with PURA and other applicable laws.

Oncor, TNMP, LCRA, and TEC requested that the confidentiality language in §25.367(l)(3) be added to §25.367(i) to expressly state that information compiled by the cybersecurity monitor or provided by the cybersecurity monitor to the commission must be treated as confidential and not subject to public disclosure under Chapter 552 of the Government Code. Oncor and TNMP stated that this addition would ensure that the confidentiality obligations under §25.367(i) comport with PURA §§39.1516(g) and 39.1516(h). Oncor, TNMP, and LCRA also requested that rule language be added to limit the recipients of the confidential information to entities or individuals such as commission staff and ERCOT and require that the information be source-anonymized.

The Integrated Utilities suggested that the rule language in §25.367(i) be revised to subject utilities to the same confidentiality standards as commission staff and the cybersecurity monitor, because confidential information may be shared in meetings conducted by the cybersecurity monitor.

*Commission Response*

The commission does not agree that additional confidentiality requirements are necessary because the proposed rule incorporates the requirements of PURA, including §§39.1516(g) and (h), which provide that information related to the cybersecurity monitor program is confidential and not subject to disclosure under Chapter 552, Government Code. The commission declines to limit recipients of confidential information to commission staff and ERCOT, or to impose specific requirements on utilities, because program participants may, with appropriate safeguards, wish to share information with one another. Further, the commission declines to require that all information be source-anonymized, because that may not be possible or desirable in all situations.

*Comments on §25.367(j) (Reporting requirements)*

TEC stated that §25.367(j) specifies that the cybersecurity monitor must submit monthly, quarterly and annual reports. To reduce production of excessive or duplicative information, TEC suggested that reporting be limited to special or periodic reports that the commission directs the cybersecurity monitor to prepare, quarterly and annual reporting, and additional reporting on an as-needed basis.

The Integrated Utilities suggested that the commission amend §25.367(j) or (k) or add a new subsection to the rule to specify that each participating utility will receive the information the cybersecurity monitor communicates to the commission and commission staff.

*Commission Response*

**Section §25.367(j) governs reports prepared by and submitted to the commission by the cybersecurity monitor. The commission does not agree that a requirement for monthly reports is duplicative or excessive. The commission declines to require that each participating utility receive the information the cybersecurity monitor communicates to the commission staff in its periodic reports. Doing so would impair informal and open communications between the cybersecurity monitor and the commission.**

*Comments on §25.367(k) (Communication between the cybersecurity monitor and the commission)*

LCRA stated that requiring the cybersecurity monitor to report to the commission and commission staff “any potential cybersecurity concerns” in §25.367(k)(2)(A) is overly broad. LCRA recommended replacing the word “potential” with “substantial” to require the cybersecurity monitor to immediately report directly to the commission and commission staff any “substantial” cybersecurity concerns. LCRA also proposed language relating to the threshold level of the concern that would trigger immediate notification.

LCRA and the Integrated Utilities stated that the proposed rule does not address the two-way flow of communication between the cybersecurity monitor and the monitored utilities contemplated by the Legislature. LCRA proposed modifying §25.367(k) to require that the cybersecurity monitor provide monitored utilities with the information it provides to the commission and commission staff.

*Commission Response*

The commission agrees with LCRA that use of the word “potential” is too broad and modifies §25.367(k)(2)(A) to provide additional guidance on cybersecurity monitor communications with the commission and commission staff.

The commission does not adopt LCRA’s proposal to require that the cybersecurity monitor provide monitored utilities with the information it provides to the commission and commission staff. Doing so would impair informal and open communications between the cybersecurity monitor and the commission.

*Comments on §25.367(l) (ERCOT's responsibilities and support role)*

TPPA stated that the proposed rule only mentions chapter 552, Government Code. TPPA supported clarifying the rule to ensure that the confidentiality obligations of PURA §39.1516(h) are extended to the language of the proposed rule.

Oncor, TNMP, and LCRA proposed adding the phrase “and must be protected in accordance with the confidentiality standards established in PURA, the ERCOT protocols, commission rules, and other applicable laws” to the provision in §25.367(l)(3) that makes ERCOT’s annual report under §25.367(l)(2) confidential and not subject to disclosure under chapter 552, Government Code.



*Commission Response*

**The commission agrees with the concerns of TPPA and LCRA on strengthening the confidentiality provisions of §25.367(l) and modifies the rule accordingly.**

*Comments on §25.367(m) (Participation in the cybersecurity monitor program)*

Oncor and TNMP recommended replacing the word “must” with “may” in §25.367(m)(1), relating to participation by monitored utilities in the cybersecurity monitor program, to reflect the voluntary aspect of the legislation that makes submission of monitored utilities’ self-assessments to the cybersecurity monitor voluntary.

*Commission Response*

**The commission declines to change the word “must” to “may” in §25.367(m)(1). SB 936 defines the term “monitored utility” and requires establishment of a cybersecurity monitor program for those entities. Although the level and nature of participation is at the discretion of the monitored utility, certain elements of the program, such as contributing to the funding of the cybersecurity monitor, are not.**

The Integrated Utilities stated that if the fee for participation in the cybersecurity monitor program is based on how many non-ERCOT utilities elect to participate, a conflict could exist between proposed §25.367(m)(2)(A)(i) that encourages non-ERCOT utilities to provide intent to participate in the program by December 1 prior to the program year, and proposed §25.367(n)(2)(B)(ii), which requires ERCOT to post the fee to participate in the program by

October 1<sup>st</sup> of the preceding program year. The Integrated Utilities recommended that this issue be addressed.

The Integrated Utilities recommended that proposed §25.367(m)(2)(B)(ii) be modified to allow proration of payments relating to participation in the cybersecurity monitor program in the event that activities under the cybersecurity monitor are suspended or impaired due to inaction of the cybersecurity monitor; or the cybersecurity monitor fails to maintain the qualifications required under this section. The Integrated Utilities also recommended that the phrase “and must notify the commission and the cybersecurity monitor, through an ERCOT-prescribed process, of its intent to discontinue participation” be added to §25.367(m)(2)(B)(iii) to reflect this requirement in PURA §36.213(3)(d)(1).

***Commission response***

The commission declines to make changes to proposed §25.367(m) in response to the comments of the Integrated Utilities. In establishing the proposed process for monitored utilities outside the ERCOT region to contribute to the cost of the cybersecurity monitor, the commission must achieve a balance among several factors, and proposed §25.367(m) properly balances those factors. First, ERCOT must have a general idea which utilities intend to participate in order to calculate an appropriate fee. Second, a non-ERCOT utility must know the approximate cost commitment being undertaken in deciding to participate. Finally, administrative costs associated with funding of the program should be minimized while still achieving program goals. The proposed rule reflects that balance appropriately. The commission modifies §25.367(m)(2) by removing an unnecessary

**sentence because the definition of monitored utility in §25.367(c)(4) includes utilities that operate solely outside the ERCOT power region that have elected to participate in the cybersecurity monitoring program.**

*Comments on §25.367(n) (Cost recovery)*

The Integrated Utilities proposed that the costs paid by a monitored utility outside of the ERCOT power region be deemed reasonable and necessary and allowed for purposes of PURA §36.213(b). The Integrated Utilities stated that the addition makes sense because the costs are beyond the control of a monitored utility; and the addition encourages participation in the cybersecurity monitor program.

OPUC responded to the Integrated Utilities' comments by stating that deeming an electric utility's costs for participation in the cybersecurity monitor program to be reasonable and necessary creates a presumption of reasonableness that is inconsistent with PURA §36.006. OPUC stated that the standard for determining whether a cost is reasonable and necessary for purposes of recovery in rates is rooted in §25.231(b), relating to cost of service, and is based on whether a cost is reasonable and necessary to provide service to the public. OPUC asserted that a monitored utility's recovery of costs in connection with participation in the cybersecurity monitor program is similar to an electric utility's recovery of costs for participating in the competitive renewable energy zone monitor program and should be treated similarly. OPUC stated that in the final order in *Commission Staff's Petition for Selection of Entities Responsible for Transmission Improvements Necessary to Deliver Renewable Energy for Competitive Renewable-Energy Zones*, Docket No. 35665 at 20 (Mar. 30, 2009), the commission allowed

recovery of costs but did not impose a presumption of reasonableness. Consistent with the precedent set in Docket No. 35665, OPUC proposed an addition to §25.367(n) to allow a monitored utility to seek recovery of its costs for participating in the program in a base rate case.

***Commission Response***

**The commission declines to address cost recovery in this new rule. The commission's existing rules on cost recovery are applicable to the costs incurred in connection with the cybersecurity coordination and cybersecurity monitor programs. In particular, §25.231(b) provides for recovery of "expenses which are reasonable and necessary to provide service to the public." Accordingly, it is unnecessary to address recovery of such costs in this rule because a utility can request recovery of its costs in a rate case and the commission can at that time review those costs and make a determination about their inclusion in rates.**

***Comments on §25.367(n) (Funding of the cybersecurity monitor)***

TEC recommended that §25.367(n) be modified to clarify that the fee paid by monitored utilities outside of the ERCOT power region will be assessed in a manner that reflects the size of the participating system. TEC suggested that the fee could be designed in a manner similar to the ERCOT system administrative fee which varies based on the load-ratio share of the entity.

***Commission response***

**The commission declines to require that the fee paid by monitored utilities reflect the size of the participating system. The rule requires ERCOT to obtain approval of the fee amount and calculation methodology from the commission's executive director. This**

**process allows for consideration of all relevant factors in determining the calculation methodology for the fee. The commission modifies §25.367(n)(2)(B) because the rule is being adopted after May 1, 2020.**

All comments, including any not specifically referenced herein, were fully considered by the commission. In adopting this section, the commission makes other modifications for the purpose of clarifying its intent.

This new section is adopted under §14.002 of the Public Utility Regulatory Act, Tex. Util. Code Ann., which provides the commission with the authority to make and enforce rules reasonably required in the exercise of its powers and jurisdiction; and specifically, PURA §31.052, which grants the commission the authority to establish a cybersecurity coordination program, and PURA §39.1516, which grants the commission authority to adopt rules as necessary to implement statute relating to the cybersecurity monitor and the cybersecurity monitor program.

Cross reference to statutes: Public Utility Regulatory Act §§14.002, 31.052, and 39.1516.

**§25.367. Cybersecurity Monitor.**

- (a) **Purpose.** This section establishes requirements for the commission's cybersecurity coordination program, the cybersecurity monitor program, the cybersecurity monitor, and participation in the cybersecurity monitor program; and establishes the methods to fund the cybersecurity monitor.
- (b) **Applicability.** This section is applicable to all electric utilities, including transmission and distribution utilities; corporations described in Public Utility Regulatory Act (PURA) §32.053; municipally owned utilities; electric cooperatives; and the Electric Reliability Council of Texas (ERCOT).
- (c) **Definitions.** The following words and terms when used in this section have the following meanings, unless the context indicates otherwise:
  - (1) **Cybersecurity monitor** -- The entity selected by the commission to serve as the commission's cybersecurity monitor and its staff.
  - (2) **Cybersecurity coordination program** -- The program established by the commission to monitor the cybersecurity efforts of all electric utilities, municipally owned utilities, and electric cooperatives in the state of Texas.
  - (3) **Cybersecurity monitor program** -- The comprehensive outreach program for monitored utilities managed by the cybersecurity monitor.
  - (4) **Monitored utility** -- A transmission and distribution utility; a corporation described in PURA §32.053; a municipally owned utility or electric cooperative that owns or operates equipment or facilities in the ERCOT power region to

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

- (d) **Selection of the Cybersecurity Monitor.** The commission and ERCOT will contract with an entity selected by the commission to act as the commission's cybersecurity monitor. The cybersecurity monitor must be independent from ERCOT and is not subject to the supervision of ERCOT. The cybersecurity monitor operates under the supervision and oversight of the commission.
- (e) **Qualifications of Cybersecurity Monitor.**
  - (1) The cybersecurity monitor must have the qualifications necessary to perform the duties and responsibilities under subsection (f) of this section.
  - (2) The cybersecurity monitor must collectively possess technical skills necessary to perform cybersecurity monitoring functions, including the following:
    - (A) developing, reviewing, and implementing cybersecurity risk management programs, cybersecurity policies, cybersecurity strategies, and similar documents;
    - (B) working knowledge of North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards and implementation of those standards; and
    - (C) conducting vulnerability assessments.

- (3) The cybersecurity monitor staff are subject to background security checks as determined by the commission.
  - (4) Every cybersecurity monitor staff member who has access to confidential information must each have a federally-granted secret level clearance and maintain that level of security clearance throughout the term of the contract.
- (f) **Responsibilities of the cybersecurity monitor.** The cybersecurity monitor will gather and analyze information and data provided by ERCOT and voluntarily disclosed by monitored utilities and cybersecurity coordination program participants to manage the cybersecurity coordination program and the cybersecurity monitor program.
- (1) **Cybersecurity Coordination Program.** The cybersecurity coordination program is available to all electric utilities, municipally owned utilities, and electric cooperatives in the state of Texas. The cybersecurity coordination program must include the following functions:
- (A) guidance on best practices in cybersecurity;
  - (B) facilitation of sharing cybersecurity information among utilities;
  - (C) research and development of best practices regarding cybersecurity;
  - (D) guidance on best practices for cybersecurity controls for supply chain risk management of cybersecurity systems used by utilities, which may include, as applicable, best practices related to:
    - (i) software integrity and authenticity;



- (ii) vendor risk management and procurement controls, including notification by a vendor of incidents related to the vendor's products and services; and
  - (iii) vendor remote access.
- (2) **Cybersecurity Monitor Program.** The cybersecurity monitor program is available to all monitored utilities. The cybersecurity monitor program must include the functions of the cybersecurity coordination program listed in paragraph (1) of this subsection in addition to the following functions:
  - (A) holding regular meetings with monitored utilities to discuss emerging threats, best business practices, and training opportunities;
  - (B) reviewing self-assessments of cybersecurity efforts voluntarily disclosed by monitored utilities; and
  - (C) reporting to the commission on monitored utility cybersecurity preparedness.
- (g) **Authority of the Cybersecurity Monitor.**
  - (1) The cybersecurity monitor has the authority to conduct monitoring, analysis, reporting, and other activities related to information voluntarily provided by monitored utilities.
  - (2) The cybersecurity monitor has the authority to request, but not to require, information from a monitored utility about activities that may be potential cybersecurity threats.

(h) **Ethics standards governing the Cybersecurity Monitor.**

- (1) During the period of a person's service with the cybersecurity monitor, the person must not:
  - (A) have a direct financial interest in the provision of electric service in the state of Texas; or have a current contract to perform services for any entity as described by PURA §31.051 or a corporation described by PURA §32.053.
  - (B) serve as an officer, director, partner, owner, employee, attorney, or consultant for ERCOT or any entity as described by PURA §31.051 or a corporation described by PURA §32.053;
  - (C) directly or indirectly own or control securities in any entity, an affiliate of any entity, or direct competitor of any entity as described by PURA §31.051 or a corporation described by PURA §32.053, except that it is not a violation of this rule if the person indirectly owns an interest in a retirement system, institution or fund that in the normal course of business invests in diverse securities independently of the control of the person; or
  - (D) accept a gift, gratuity, or entertainment from ERCOT, any entity, an affiliate of any entity, or an employee or agent of any entity as described by PURA §31.051 or a corporation described by PURA §32.053.
- (2) The cybersecurity monitor must not directly or indirectly solicit, request from, suggest, or recommend to any entity, an affiliate of any entity, or an employee or agent of any entity as described by PURA §31.051 or a corporation described by

PURA §32.053, the employment of a person by any entity as described by PURA §31.051 or a corporation described by PURA §32.053 or an affiliate.

- (3) The commission may impose post-employment restrictions for the cybersecurity monitor and its staff.
  
- (i) **Confidentiality standards.** The cybersecurity monitor 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.
  
- (j) **Reporting requirement.** All reports prepared by the cybersecurity monitor must reflect the cybersecurity monitor's independent analysis, findings, and expertise. The cybersecurity monitor must prepare and submit to the commission:
  - (1) monthly, quarterly, and annual reports; and
  - (2) periodic or special reports on cybersecurity issues or specific events as directed by the commission or commission staff.
  
- (k) **Communication between the Cybersecurity Monitor and the commission.**
  - (1) The personnel of the cybersecurity monitor may communicate with the commission and commission staff on any matter without restriction consistent with confidentiality requirements.
  - (2) The cybersecurity monitor must:

- (A) immediately report directly to the commission and commission staff any cybersecurity concerns that the cybersecurity monitor believes would pose a threat to continuous and adequate electric service or create an immediate danger to the public safety, and notify the affected utility or utilities of the information reported to the commission or commission staff;
  - (B) regularly communicate with the commission and commission staff, and keep the commission and commission staff apprised of its activities, findings, and observations;
  - (C) coordinate with the commission and commission staff to identify priorities; and
  - (E) coordinate with the commission and commission staff to assess the resources and methods for cybersecurity monitoring, including consulting needs.
- (l) **ERCOT's responsibilities and support role.** ERCOT must provide to the cybersecurity monitor any access, information, support, or cooperation that the commission determines is necessary for the cybersecurity monitor to perform the functions described by subsection (f) of this section.
- (1) ERCOT must conduct an internal cybersecurity risk assessment, vulnerability testing, and employee training to the extent that ERCOT is not otherwise required to do so under applicable state and federal cybersecurity and information security laws.

- (2) ERCOT must submit an annual report to the commission on ERCOT's compliance with applicable cybersecurity and information security laws by January 15 of each year or as otherwise determined by the commission.
  - (3) Information submitted in the report under paragraph (2) of this subsection is confidential and not subject to disclosure under chapter 552, Government Code, and must be protected in accordance with the confidentiality standards established in PURA, the ERCOT protocols, commission rules, and other applicable laws.
- (m) **Participation in the cybersecurity monitor program.**
  - (1) A transmission and distribution utility, a corporation described in PURA §32.053, and a municipally owned utility or electric cooperative that owns or operates equipment or facilities in the ERCOT power region to transmit electricity at 60 or more kilovolts must participate in the cybersecurity monitor program.
  - (2) An electric utility, municipally owned utility, or electric cooperative that operates solely outside the ERCOT power region may elect to participate in the cybersecurity monitor program.
    - (A) An electric utility, municipally owned utility, or electric cooperative that elects to participate in the cybersecurity monitor program must annually:
      - (i) file with the commission its intent to participate in the program and to contribute to the costs of the cybersecurity monitor's activities in the project established by commission staff for this purpose; and
      - (ii) complete and submit to ERCOT the participant agreement form available on the ERCOT website to furnish information necessary

to determine and collect the monitored utility's share of the costs of the cybersecurity monitor's activities under subsection (n) of this section.

- (B) The cybersecurity monitor program year is the calendar year. An electric utility, municipally owned utility, or electric cooperative that elects to participate in the cybersecurity monitor program must file its intent to participate and complete the participant agreement form under subparagraph (A) of this subsection for each calendar year that it intends to participate in the program.
- (i) Notification of intent to participate and a completed participant agreement form may be submitted at any time during the program year, however, an electric utility, municipally owned utility, or electric cooperative that elects to participate in an upcoming program year is encouraged to complete these steps by December 1 prior to the program year in order to obtain the benefit of participation for the entire program year.
  - (ii) The cost of participation is determined on an annual basis and will not be prorated.
  - (iii) A monitored utility that operates solely outside of the ERCOT power region may discontinue its participation in the cybersecurity monitor program at any time but is required to pay the annual cost of participation for any calendar year in which the monitored utility submitted a notification of intent to participate.

- (3) Each monitored utility must designate one or more points of contact who can answer questions the Cybersecurity Monitor may have regarding a monitored utility's cyber and physical security activities.
- (n) **Funding of the Cybersecurity Monitor.**
- (1) ERCOT must use funds from the rate authorized by PURA §39.151(e) to pay for the cybersecurity monitor's activities.
  - (2) A monitored utility that operates solely outside of the ERCOT power region must contribute to the costs incurred for the cybersecurity monitor's activities.
    - (A) On an annual basis, ERCOT must calculate the non-refundable, fixed fee that a monitored utility that operates solely outside of the ERCOT power region must pay in order to participate in the cybersecurity monitor program for the upcoming calendar year.
    - (B) ERCOT must file notice of the fee in the project designated by the commission for this purpose and post notice of the fee on the ERCOT website by October 1 of the preceding program year.
    - (C) Before filing notice of the fee as required by paragraph (2)(B) of this subsection, ERCOT must obtain approval of the fee amount and calculation methodology from the commission's executive director.

This agency certifies that the adoption has been reviewed by legal counsel and found to be a valid exercise of the agency's legal authority. It is therefore ordered by the Public Utility Commission of Texas that §25.367 relating to cybersecurity monitor is hereby adopted with changes to the text as proposed.

Signed at Austin, Texas the 14<sup>th</sup> day of May 2020.

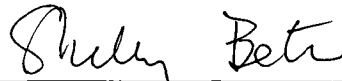
**PUBLIC UTILITY COMMISSION OF TEXAS**



DEANN T. WALKER, CHAIRMAN



ARTHUR C. D'ANDREA, COMMISSIONER



SHELLY BOTKIN, COMMISSIONER