Control Number: 49819

Item Number: 3

Addendum StartPage: 0

OPEN MEETING COVER SHEET
RULEMAKING

MEETING DATE:	December 13, 2019
DATE DELIVERED:	December 6, 2019
AGENDA ITEM NO.:	18
CAPTION:	Project No. 49819 – Rulemaking to Relating to Cybersecurity Monitor
ACTION REQUESTED:	Discussion and possible action with respect to Proposal for Publication

Distribution List:
Commissioners' Offices (6)
Urban, John Paul
Corona, Connie
Gleeson, Thomas
Phillips, Michael
Central Records (Open Meeting Notebook)
Rogas, Keith (2)
Hunter, Tom (5)
Journeay, Stephen
Agenda
Burch, Chris
Tietjen, Darryl (2)
Long, Mick (2)
Zerwas, Rebecca (2)
Benter, Tammy (2)
Gonzalez, Andrea
Woltersdorf, Paytyn
Hoke, Mike
Mueller, Paula

3

Public Utility Commission of Texas

Memorandum

To: Chairman DeAnn T. Walker
Commissioner Arthur C. D'Andrea
Commissioner Shelly Botkin

From: Chuck Bondurant, Critical Infrastructure Security and Risk Management
Therese Harris, Infrastructure Division

Date: December 6, 2019

Re: Open Meeting, December 13, 2019—**Agenda Item # 18**
Project No. 49819 – *Rulemaking Relating to Cybersecurity Monitor*

Commissioners,

Attached for your review and consideration is staff's proposal for publication in Project No. 49819, *Rulemaking Relating to Cybersecurity Monitor*. This rulemaking proposes new §25.367, relating to cybersecurity monitor.

The proposed new 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 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 Senate Bill 936, relating to cybersecurity monitor for certain electric utilities, 86th Legislature, Regular Session.

Please contact Chuck Bondurant at chuck.bondurant@puc.texas.gov or 512-936-7280; or Therese Harris at therese.harris@puc.texas.gov or 512-936-7378 with questions.

PROJECT NO. 49819

RULEMAKING RELATING TO CYBERSECURITY MONITOR	§ § §	**PUBLIC UTILITY COMMISSION OF TEXAS**

(STAFF RECOMMENDATION)
PROPOSAL FOR PUBLICATION OF NEW §25.367
FOR CONSIDERATION AT THE DECEMBER 13, 2019 OPEN MEETING

The Public Utility Commission of Texas (commission) proposes new §25.367, relating to cybersecurity monitor. The proposed new 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 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 Senate Bill 936, relating to cybersecurity monitor for certain electric utilities, 86th Legislature, Regular Session.

Growth Impact Statement

The agency provides the following governmental growth impact statement for the proposed rule, as required by Texas Government Code §2001.0221. The agency has determined that for each year of the first five years that the proposed rule is in effect, the following statements will apply:

(1) the proposed rule will not create a government program beyond those required by statute and will not eliminate a government program;

(2) implementation of the proposed rule will not require the creation of new employee positions and will not require the elimination of existing employee positions;

(3) implementation of the proposed rule will not require an increase and will not require a decrease in future legislative appropriations to the agency;

(4) the proposed rule will not require an increase and will not require a decrease in fees paid to the agency;

(5) the proposed rule will not create a new regulation;

(6) the proposed rule will not expand an existing regulation;

(7) the proposed rule will not change the number of individuals subject to the rule's applicability; and

(8) the proposed rule will not affect this state's economy.

Fiscal Impact on Small and Micro-Businesses and Rural Communities

There is no adverse economic effect anticipated for small businesses, micro-businesses, or rural communities as a result of implementing the proposed rule. Accordingly, no economic impact statement or regulatory flexibility analysis is required under Texas Government Code §2006.002(c).

Takings Impact Analysis

The commission has determined that the proposed rule will not be a taking of private property as defined in chapter 2007 of the Texas Government Code.

Fiscal Impact on State and Local Government

Chuck Bondurant, Director of Critical Infrastructure Security and Risk Management, has determined that for the first five-year period the proposed rule is in effect, there will be no fiscal

implications for the state or for units of local government under Texas Government Code §2001.024(a)(4) as a result of enforcing or administering the rule.

Public Benefits

Mr. Bondurant has also determined that for each year of the first five years the proposed rule is in effect, the anticipated public benefits expected as a result of the adoption of the proposed rule will be collaboration among the commission, electric utilities, electric cooperatives, municipally owned electric utilities, and the Electric Reliability Council of Texas (ERCOT) regarding efforts to secure critical electric infrastructure from cyber vulnerabilities. The probable economic cost for ERCOT to implement PURA §39.1516, added by SB 936 in the 86th Legislature, will be funding the cybersecurity monitor's activities from the rate authorized by PURA §39.151(e). For a monitored utility operating in the ERCOT power region, the cost of the cybersecurity monitor's activities will be paid by the ERCOT system administration fee. This fee is unlikely to increase as a result of the implementation of PURA §39.1516. The probable economic cost for an electric utility, electric cooperative, or municipally owned electric utility operating solely outside the ERCOT power region that elects to participate in the cybersecurity monitor program is the cost of their contribution to the costs incurred for the cybersecurity monitor's activities. There is no anticipated economic cost for an electric utility, electric cooperative, or municipally owned electric utility to participate in the statewide cybersecurity coordination program.

Local Employment Impact Statement

For each year of the first five years the proposed section is in effect, there should be no effect on a local economy; therefore, no local employment impact statement is required under Texas Government Code §2001.022.

Costs to Regulated Persons

Texas Government Code §2001.0045(b) does not apply to this rulemaking, because the Public Utility Commission is expressly excluded under subsection §2001.0045(c)(7).

Public Hearing

The commission staff will conduct a public hearing on this rulemaking, if requested in accordance with Texas Government Code §2001.029, at the commission's offices located in the William B. Travis Building, 1701 North Congress Avenue, Austin, Texas 78701 on March 4, 2020 at 9:00 AM. The request for a public hearing must be received by February 10, 2020. If no request for a public hearing is received and the commission staff cancels the hearing, it will make a filing in this project prior to the scheduled date to cancel the hearing.

Public Comments

Initial comments on the proposed rule may be filed with the commission's filing clerk at 1701 North Congress Avenue, Austin, Texas or mailed to P.O. Box 13326, Austin, TX 78711-3326, by January 27, 2020. Reply comments may be submitted by February 10, 2020. Sixteen copies of comments on the proposed rule are required to be filed by §22.71(c) of 16 Texas Administrative Code. Comments should be organized in a manner consistent with the

organization of the proposed rule. The commission invites specific comments regarding the costs associated with, and benefits that will be gained by, implementation of the proposed rule. The commission will consider the costs and benefits in deciding whether to modify the proposed rule on adoption. All comments should refer to project number 49819.

Statutory Authority

This new rule is proposed under §14.002 of the Public Utility Regulatory Act, Tex. Util. Code Ann. (West 2016 and Supp. 2017) (PURA), 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 (CSM)** -- 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 CSM.

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

(e) **Qualifications of CSM.**

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

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

(A) developing, reviewing, and implementing cybersecurity risk management programs, cybersecurity policies, cybersecurity strategies, and similar governance 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 CSM director and staff are subject to background security checks as determined by the commission.

(4) The CSM director and every CSM 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 CSM.** The CSM will gather and analyze information and data as needed 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 and 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 CSM.**

(1) The CSM has the authority to conduct monitoring, analysis, reporting, and related activities but has no enforcement authority.

(2) The CSM has the authority to request information from a monitored utility about activities that may be potential cybersecurity threats.

(3) The 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.

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

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

(A) have a specific interest in the commission's regulation and must not 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 CSM director or a CSM staff member 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 CSM and its staff.

(i) **Confidentiality standards.** 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.

(j) **Reporting requirement.** All reports prepared by the CSM must reflect the CSM's independent analysis, findings, and expertise. The CSM 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 CSM and the commission.**

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

(2) The CSM must:

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

(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 CSM any access, information, support, or cooperation that the commission determines is necessary for the CSM 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.

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

(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 CSM'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 CSM'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 elected to participate under subsection (m)(2) 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.

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

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

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

(i) For the 2020 program year, ERCOT must file and post notice of the fee to participate in the program by May 1, 2020.

(ii) Beginning with the 2021 program year, ERCOT must file and post notice of the fee to participate in the program 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 proposal has been reviewed by legal counsel and found to be within the agency's legal authority to adopt.

ISSUED IN AUSTIN, TEXAS ON THE _____ DAY OF _____ 2019 BY THE PUBLIC UTILITY COMMISSION OF TEXAS
ANDREA GONZALEZ