CHAPTER 25. SUBSTANTIVE RULES APPLICABLE TO ELECTRIC SERVICE PROVIDERS.

Subchapter O. UNBUNDLING AND MARKET POWER. Division 2. Independent Organizations

§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

(D) 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.