

- SUBJECT:** Establishing a cybersecurity monitor program for certain electric utilities
- COMMITTEE:** State Affairs — committee substitute recommended
- VOTE:** 9 ayes — Phelan, Guerra, Harless, Holland, Hunter, P. King, Raymond, Smithee, Springer
- 0 nays
- 4 absent — Hernandez, Deshotel, Parker, E. Rodriguez
- SENATE VOTE:** On final passage, April 4 — 31-0
- WITNESSES:** *On House companion bill, HB 3377:*  
For — (*Registered, but did not testify:* Isaac Albarado, AEP Texas; Erika Akpan, Association of Electric Companies of Texas; Tami Miller, CenterPoint Energy; Bill Lauderback, Lower Colorado River Authority; Katie Coleman, Texas Association of Manufacturers; Evan Autry, Texas Electric Cooperatives; Russell T. Keene, Texas Public Power Association)
- Against — None
- On — (*Registered, but did not testify:* Cheryl Mele, Electric Reliability Council of Texas; Thomas Gleeson, Public Utility Commission)
- BACKGROUND:** Some have called for a framework for a collaborative partnership between the Public Utility Commission, the Electric Reliability Council of Texas, and electric utilities to coordinate efforts to secure critical electric infrastructure from cyber vulnerabilities.
- DIGEST:** CSSB 936 would require the Public Utility Commission (PUC) and the Electric Reliability Council of Texas (ERCOT) to contract with an entity to act as PUC's cybersecurity monitor to:
- manage a comprehensive cybersecurity outreach program for monitored utilities;

- meet regularly with monitored utilities to discuss emerging threats, best business practices, and training opportunities;
- review self-assessments of cybersecurity efforts voluntarily disclosed by monitored utilities;
- research and develop best business practices on cybersecurity; and
- report to PUC on monitored utility cybersecurity preparedness.

Monitored utilities would include:

- transmission and distribution utilities;
- wholesale retailers of electric energy on behalf of river authorities; and
- certain municipally owned utilities or electric cooperatives that operated in or solely outside the ERCOT power region.

The bill would require PUC, on its own motion or on the petition of an electric utility, to allow the utility to recover costs incurred in connection with the cybersecurity monitor program.

An electric utility, municipally owned utility, or electric cooperative that operated solely outside the ERCOT power region could elect to participate in the cybersecurity monitor program or to discontinue participation. PUC would have to establish procedures for a utility or cooperative to notify PUC, ERCOT, and the monitor that it elected to participate or discontinue participation. PUC would have to adopt a mechanism to require a utility or cooperative that elected to participate to contribute to costs incurred by ERCOT under the bill.

The cybersecurity monitor would operate under the supervision and oversight of PUC. ERCOT would have to provide the monitor any access, information, support, and cooperation that PUC determined was necessary for the monitor to perform required functions under the bill. ERCOT would have to use funds from administrative fees authorized under law to pay for the monitor's activities.

The bill would not grant enforcement authority to the cybersecurity

monitor or authorize PUC to delegate its enforcement authority to the monitor. PUC could enforce the bill in the manner provided by law; the bill would not grant enforcement authority to PUC beyond what is explicitly provided for under current law.

The staff of the cybersecurity monitor could communicate with PUC about any cybersecurity information without restriction. PUC staff would have to maintain the confidentiality of the information and could not disclose information in an open meeting or through a response to a public information request. Information written, produced, collected, assembled, or maintained under the bill would be confidential and not subject to disclosure under public information laws. A governmental body would not be required to conduct an open meeting to deliberate a matter related to the cybersecurity monitor program.

The bill would apply the monitoring program to electric utilities, certain river authorities, or electric cooperatives with respect to the implementation of customer choice. PUC's jurisdiction over municipally owned utilities and electric cooperatives would be expanded to include the evaluation and monitoring of cybersecurity preparedness related to the program.

To the extent of any conflict, CSSB 936 would prevail over another bill of the 86th Legislature, Regular Session, 2019, relating to nonsubstantive additions to and correction in enacted codes.

The bill would take effect September 1, 2019.