

BILL ANALYSIS

H.B. 3377
By: Hernandez
State Affairs
Committee Report (Unamended)

BACKGROUND AND PURPOSE

Increasing incidence and scale of threats to cybersecurity are a widely discussed public concern. Uncertainty regarding the impact these threats could pose to electric utilities, which often rely on intricate computer networks to operate, is a particular source of apprehension. Because the security and safety of electric utility assets is a prime concern for the economic and physical well-being of the state, H.B. 3377 seeks to develop a framework for collaboration between the Public Utility Commission of Texas, electric utilities, and ERCOT regarding efforts to secure critical electric infrastructure from cyber vulnerabilities by providing for a cybersecurity monitor for these utilities.

CRIMINAL JUSTICE IMPACT

It is the committee's opinion that this bill does not expressly create a criminal offense, increase the punishment for an existing criminal offense or category of offenses, or change the eligibility of a person for community supervision, parole, or mandatory supervision.

RULEMAKING AUTHORITY

It is the committee's opinion that rulemaking authority is expressly granted to the Public Utility Commission of Texas in SECTION 3 of this bill.

ANALYSIS

H.B. 3377 amends the Utilities Code to require the Public Utility Commission of Texas (PUC) and the independent organization certified to perform certain functions related to the market structure of the electric utility industry to contract with an entity selected by the PUC to act as its cybersecurity monitor for specified purposes. The bill requires the certified independent organization to provide to the cybersecurity monitor any access, information, support, and cooperation that the PUC determines is necessary for the monitor to perform its functions and to use funds from the system administration fee charged to wholesale buyers and sellers to pay for the monitor's activities.

H.B. 3377 authorizes an electric utility, municipally owned utility, or electric cooperative that operates solely outside the ERCOT power region to elect to participate in the cybersecurity monitor program or to discontinue participation. The bill requires the PUC to adopt rules establishing procedures for such an entity to provide notice of the fact that the entity elects to participate or to discontinue participation and establishing a mechanism to require an entity that elects to participate to contribute to the costs incurred by the independent organization in relation to the program. The bill requires the cybersecurity monitor to operate under PUC supervision and oversight.

H.B. 3377 authorizes the cybersecurity monitor's staff to communicate with PUC staff about any cybersecurity information without restriction and requires PUC staff to maintain the information's confidentiality. The bill prohibits PUC staff from disclosing information obtained

under the bill's provisions relating to the cybersecurity monitor in an open meeting or through a response to a public information request and makes certain of that information written, produced, collected, assembled, or maintained by the PUC confidential and exempt from disclosure under state public information law. The bill expressly does not require a governmental body to conduct an open meeting to deliberate certain cybersecurity matters.

H.B. 3377 requires the PUC to adopt rules as necessary to implement the bill's provisions providing for a cybersecurity monitor and authorizes the PUC to enforce those provisions in the manner provided by the Public Utility Regulatory Act. The bill expressly does not grant enforcement authority to the cybersecurity monitor or authorize the PUC to delegate its enforcement authority to the cybersecurity monitor and expressly does not grant enforcement authority to the PUC beyond authority explicitly provided for in that act. The bill clarifies the applicability of the cybersecurity monitor program with respect to a qualifying river authority, a municipally owned utility, or an electric cooperative and with respect to the implementation of customer choice by an electric utility.

H.B. 3377 requires the PUC, on its own motion or on the petition of an electric utility, to allow the electric utility to recover reasonable and necessary costs incurred in connection with activities under the cybersecurity monitor program. That provision does not apply to an electric utility that operates solely outside of ERCOT and that has not elected to participate in the program.

H.B. 3377 expands the jurisdiction of the PUC over municipally owned utilities and electric cooperatives to include evaluating and monitoring the cybersecurity preparedness of certain municipally owned utilities and electric cooperatives.

EFFECTIVE DATE

September 1, 2019.