



1-888-440-3311

P.O. Box 1937, Hughesville, MD 20637

www.smeco.coop

People. Power. Progress.

March 6, 2023

SB 800: Public Service Commission – Cybersecurity Staffing and Assessments (Critical Infrastructure Cybersecurity Act of 2023)

Committee: Senate Education, Energy and the Environment

Position: OPPOSED

Southern Maryland Electric Cooperative (SMECO), a member-owned electric cooperative based in Hughesville that provides electricity to more than 170,000 member accounts in Charles, St. Mary's, Calvert and southern Prince George's County, opposes Senate Bill 800. This bill requires the Public Service Commission (PSC) to include one or more employees that are experts in cybersecurity on its staff for specified purposes. In supervising and regulating public service companies, PSC must also consider the protection of a public service company's infrastructure against cyberattack threats. Each public service company, except common carriers and telephone companies, must take specified actions related to cybersecurity, including contracting with a third party every two years beginning in 2024 for an assessment of operational technology and information technology (IT) devices based on specified security frameworks and submitting related information to PSC. PSC is required to conduct related evaluations of the assessments for three consecutive years starting with October 1, 2023, and then every two years thereafter.

SMECO opposes SB 800 because the bill is redundant of current federal cybersecurity requirements. The bill would require significant additions of new staff, documentation, configuration changes and management of distribution level assets at a cost to the Cooperative's ratepayers. The bill also requires that utilities adopt a zero-trust cybersecurity approach for on-premises services, which is duplicative of our current practice as SMECO currently adopts the principle of least privilege and zero-trust approach through our environment, specifically in the SCADA environment through CIP.

For more information, contact: Natalie Cotton, SMECO
Government Affairs & Community Relations Director
240-393-3919 • Natalie.cotton@smeco.coop

SMECO recognizes the importance of implementing effective cybersecurity controls consistent with established and evolving security standards to protect critical infrastructure and maintain safe, reliable, and affordable energy delivery. The rapidly evolving nature of cybersecurity threats poses unique challenges for the critical infrastructure community, including utilities, and warrants careful consideration.

While we appreciate the need to ensure that cybersecurity tools and approaches keep pace with new cyber threats, the General Assembly should also keep in mind that the utility industry has not been idle. SMECO is constantly improving their cybersecurity programs to stay ahead of threats pursuant to federal cybersecurity requirements and advances in the industry.

The bill would also require that at least once every other year that utilities contract with a third party to conduct an assessment of operational technology and information technology devices based on National Institute of Standards and Technology (NIST) frameworks. The PSC currently requires utilities to present their cybersecurity posture to them every three years. We respectfully ask that utilities be allowed to continue to align our programs with federal industry standards and requirements that incorporate strong cybersecurity controls and best practices which will be overseen by the PSC without the use of a third-party assessor. A third-party expert certification approach will introduce additional costs and may result in unintended risks such as inconsistencies with third-party evaluators. A key factor in successful compliance programs is consistency—relying solely on third parties to perform compliance verifications may result in divergent compliance monitoring approaches and interpretations.

SMECO believes that the current federal regulations via FERC, NERC and Reliability First, which deals with Critical Infrastructure Protection (CIP) adequately addresses the bill's requirements. For that and the reasons explained above, SMECO urges the committee to give an unfavorable report to SB 800.