March 28, 2024

112 West Street
Annapolis, MD 21401

UNFAVORABLE - House Bill 1420 - Cybersecurity - Office of People's Counsel, Public Service Companies, Public Service Commission, and Maryland Cybersecurity Council

Potomac Electric Power Company (Pepco) and Delmarva Power & Light Company (Delmarva Power) respectfully oppose **House Bill 1420- Cybersecurity - Office of People's Counsel, Public Service Companies, Public Service Commission, and Maryland Cybersecurity Council.** This legislation requires the Public Service Commission (PSC) to incorporate "cyber resilience" into existing regulations pertaining to service quality and reliability standards of electric companies, adds an additional requirement for third-party assessments of public service companies' operational technology and information technology devices and establishes various definitions related to cybersecurity and cybersecurity vulnerabilities in existing State law. The bill also explicitly authorizes the Office of People's Counsel (OPC) to hire experts in the field of cybersecurity.

In the 2023 legislative session, the General Assembly enacted House Bill 969 - Critical Infrastructure Cybersecurity Act of 2023. The legislation added cyber security staff to the Maryland Public Service Commission (PSC) and requires them to establish minimum cyber security standards for public utilities. Specifically, the legislation: (1) requires the PSC to include one or more cybersecurity experts on its Staff to advise the Commission and perform certain duties; (2) requires the PSC to establish minimum cybersecurity standards and best practices for regulated entities and share cybersecurity related information/best practices with municipal electric utilities; (3) requires the PSC to conduct and submit an evaluation of the public service companies' assessments to Maryland Department of Information Technology ("DoIT") Office of Security Management and the Maryland Department of Emergency Management ("MDEM") and (4) requires public service companies to adopt and implement cybersecurity standards and conduct assessments, and report cyber security incidents.

Pepco and Delmarva Power are concerned that House Bill 1420 expands and potentially conflicts with the 2023 statute which is currently being implemented through a rulemaking process at the PSC. Since House Bill 969 was enacted into law, the PSC has been working with the Cybersecurity Reporting Work Group, a group established by the PSC in 2017 to work on a framework for future cybersecurity reporting. The group has met several times to discuss implementation but has not reached consensus on several issues raised by the public service companies, namely scope of proposed cybersecurity regulations, cybersecurity incident reporting, zero trust implementation, confidentiality and compliance and enforcement, among other things.

Pepco and Delmarva Power are concerned that, as written, House Bill 1420 includes definitions such as “zero-trust” and others that conflict with current statutes and regulations. Additionally, the definition of “critical software” is overly broad and changes the scope for assessments defined in the Critical Infrastructure Cybersecurity Act. Pepco and Delmarva Power support aligning the definitions and standards with an existing cybersecurity framework (NIST-CSF) and should be not prescriptive to avoid introducing operational and security issues for non-federally regulated assets. A zero-trust cybersecurity approach should be defined as a public utility company’s strategy to incorporate zero-trust concepts into its risk management program. Pepco and Delmarva Power respectfully ask that the process underway to adopt regulations for House Bill 969 be finalized before we consider additional legislation.

We understand that the amended bill requires a third-party assessment of operational technology (OT) and IT devices that “analyzes critical software used in OT and IT devices. There are significant concerns with the purpose of the requirement as a risk reducing element, in addition to the technical feasibility, cost, level of effort, and timeframe required to perform. The bill as drafted does not provide a definition for “analyzes critical software.” In software development, analyze refers to the methods used for software diagnosis and testing, improving qualify and correctness, encompassing reliability, security and performance. Software customers cannot obtain code for commercial software making it impossible to analyze. Even if technically feasible, assessing at a device level could create unintended harm to the functionality of the device in real-time which could disrupt the stability of the IT and OT systems. The scope as written would include all IT and OT devices which for each utility would amount to tens of thousands of devices – each of which could have multiple instances of software. An analysis would first require categorizing software based on the “critical software” definition which has not yet been applied to critical infrastructure – even at the federal level.

Federal guidance for security measures for critical software reference the NIST CSF and NIST SP 800-53 for recommended security measures and controls. “Analyzing critical software” is not included in either. Instead, these risks are managed through the following measures and controls (which does not include analyzing critical software) use of multi-factor authentication (MFA), identify and access management, network segmentation, data inventory, encryption, backups, software inventory, patch management, configuration management, logging and monitoring, continuous monitoring, endpoint protection, network security protection, security awareness training, and incident response training.

Public service companies are already required, based on the Maryland Critical Infrastructure Cybersecurity Act, to conduct a third-party assessment of IT and OT devices based on the Cybersecurity and Infrastructure Security Agencies Cross-Sector Cybersecurity Performance Goal (CISA CPG) or NIST CSF frameworks. Such an assessment would identify whether or not a company has a program in place to manage software risk. As such, this provision is unnecessary if the intent of the legislation is to ensure that public service companies are identifying and managing such risk.

Public service companies are already required to demonstrate their cyber resiliency based upon the in-person confidential cybersecurity briefings provided to the PSC by the public service companies. In addition, the new third-party assessment requirement would identify many of the factors included in the cyber resilience definition given that the fundamental purpose of applying a cybersecurity framework is to ensure resiliency and recovery. Incorporating the term into a performance metric for consistent application across public service companies would be almost impossible and would increase compliance costs with little apparent benefit to the ratepayers.

Pepco and Delmarva Power are committed to continuing to work with the bill sponsor and all stakeholders on the aforementioned concerns, but respectfully asks the Committee to issue an unfavorable report on House Bill 1420.

Contact:
Anne Klase
Senior Manager, State Affairs
240-472-6641
Anne.klase@exeloncorp.com

Katie Lanzarotto
Manager, State Affairs
410-935-3790
Kathryn.lanzarotto@exeloncorp.com