HB1420 Kaiser Testimony - Senate.pdf
Uploaded by: Anne Kaiser
Position: FAV

ANNE R. KAISER
Legislative District 14
Montgomery County

Health and Government
Operations Committee

House Chair
Joint Committee on Cybersecurity,
Information Technology and
Biotechnology

The Maryland House of Delegates
6 Bladen Street, Room 425
Annapolis, Maryland 21401
301-858-3036 · 410-841-3036
800-492-7122 *Ext.* 3036
Fax 301-858-3060 · 410-841-3060
Anne.Kaiser@house.state.md.us

THE MARYLAND HOUSE OF DELEGATES
ANNAPOLIS, MARYLAND 21401

Testimony in Support of HB1420: Cybersecurity - Office of People's Counsel, Public Service Companies, Public Service Commission, and Maryland Cybersecurity Council
March 28, 2024

Chair Feldman and esteemed members of the Education, Energy, and the Environment Committee, it is my pleasure to come before you and offer testimony in favor of **House Bill 1420: Cybersecurity - Office of People's Counsel, Public Service Companies, Public Service Commission, and Maryland Cybersecurity Council**. As amended, this bill codifies the Office of People's Counsel's (OPC) ability to retain cybersecurity expertise as needed and sets standard definitions of critical software, supply chain risk, zero-trust, cyber resilience, and critical infrastructure.

This proposed legislation stems from a 2021 report from the Office of the Attorney General and the Maryland Cybersecurity Council. This report, authored by Laura Corcoran, an NSA Fellow, identified several recommendations to improve the security, resilience, and reliability of Maryland's electric distribution systems, known as "the electric grid." Some of the broader recommendations from the report were adopted last year, while other important standards and definitions were omitted. As our electric grid continues to undergo major transformations and our dependence on the electric grid grows, cybersecurity measures must be updated regularly. The definitions and standards set in this bill are critical to the successful modernization of our electric grid, a vital component of Maryland's strategy to meet our ambitious clean energy goals. The Public Service Commission, responsible for regulating electric utilities and evaluating the cybersecurity practices of utility companies, has advised that the updated regulations can be implemented within the current budget.

The industry has expressed concern that this bill will conflict with federal regulations. However, the scope of this legislation is specific to distribution systems, which do not fall under federal jurisdiction, and have been left to the states to regulate. Additionally, this bill will have no bearing on the cybersecurity report mandated by last year's legislation, which is due by July 1st of this year and every two years thereafter. The changes made in this bill would not take effect until October 1st, well after the report submission deadline and well before the next deadline. According to industry experts on the MD Cybersecurity Council, the proposed legislation is well within Maryland's jurisdiction and will have no bearing on the implementation of last year's bill.

I urge a favorable report on **House Bill 1420: Cybersecurity - Office of People's Counsel, Public Service Companies, Public Service Commission, and Maryland Cybersecurity Council.** Thank you.

Von Lehmen__Staff Maryland Cybersecurity Council__
Uploaded by: Greg Lehmen
Position: FWA

FAVORABLE WITH AMENDMENT

TESTIMONY PRESENTED TO THE
SENATE COMMITTEE ON HEALTH, ENERGY, AND THE ENVIRONMENT

HB 1420 (CYBERSECURITY – OFFICE OF PEOPLE'S COUNSEL, PUBLIC SERVICE COMPANIES, PUBLIC SERVICE COMMISSION, AND MARYLAND CYBERSECURITY COUNCIL)

DR. GREG VON LEHMEN
STAFF, MARYLAND CYBERSECURITY COUNCIL

POSITION: SUPPORT
MARCH 28, 2024

Mr. Chair, Madam Vice Chair, and members of the committee, thank you for the opportunity to testify. I am Dr. Greg von Lehmen, staff to the Maryland Cybersecurity Council, a statutory body chaired by Attorney General Brown.

As background, the Council benefitted in 2021 from a report on the electric grid serving Maryland.[1] This report was authored by an NSA employee who worked for one year in the Office of the Attorney General as a researcher for the Council. Altogether, the report made 29 recommendations, the most substantive of which were included in HB 969 (2023) which passed the General Assembly and was signed by the Governor last year. There is currently a rulemaking underway (RM 76) to implement the provisions of that bill.

House Bill 1420 aims to implement several of the report's recommendations. This includes the bill's provision for the Office of People's Counsel (OPC) to hire and retain cybersecurity expertise as necessary. It also includes the bill's provisions that aim to address the absence of definitions in Maryland law for "supply chain risk" and "critical infrastructure" and defining "critical software" as a separate category of software for the security assessments required by law, and specifying "cyber resilience" as a service and reliability objective.

Given the role of OPC and the importance of cybersecurity, it is appropriate to call out cybersecurity as expertise that OPC may hire as necessary. Further, I can see no downside in adding definitions of "supply chain risk" and "critical

[1] Corcoran, L. (2021, December) Cybersecurity and the Maryland Electric Grid. Maryland Cybersecurity Council. https://www.umgc.edu/content/dam/umgc/documents/md-cybersecurity-council/cybersecurity-and-the-maryland-electric-grid.pdf

infrastructure" to the law. The definitions in the bill have the virtue of being very close to or exactly conforming with definitions provided by the National Institute for Standards and technology (NIST).[2]

I would concur with the position of the Public Service Commission that the bill's provisions regarding "critical software" and "cybersecurity resilience" are materially met, if not specifically called out, by HB 969's (2023) adoption of the cross-sector cybersecurity performance goals recommended by the Cybersecurity and Critical Infrastructure Security Agency (CISA). Consequently, I discern no harm or infidelity to the report's recommendations by removing these provisions by amendment.

Thank you for the opportunity to testify.

[2] National Institute for Standards and Technology Computer Security Resource Center. Glossary. https://csrc.nist.gov/glossary

BGE_EEE_OPP_House Bill 1420 - Cybersecurity - Offi
Uploaded by: Dytonia Reed
Position: UNF

bge
AN EXELON COMPANY

Position Statement

Oppose
Education, Energy, and the Environment
3/28/2024

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

Baltimore Gas and Electric Company (BGE) opposes *House Bill 1420*. *House Bill 1420* as amended authorizes the Office of People's Counsel (OPC) to hire an expert with cybersecurity expertise to ensure utility compliance with cybersecurity minimum standards. It adds to the requirements for a third-party assessment of public service company critical software used in operational technology and information technology devices and requires public service companies submit to the Maryland Public Service Commission (Commission) a certification of the public service company's compliance with standards in the assessment. Also, *House Bill 1420* requires the Commission to include cyber resilience in its cybersecurity regulations.

BGE opposes *House Bill 1420* for several reasons. First, the legislation is inconsistent with the 2023 Critical Infrastructure Cybersecurity Act (House Bill 969).

The legislation conflicts with House Bill 969 that was enacted last year. House Bill 969 required regulated entities to conduct a third-party assessment and submit an evaluation of the public service companies' assessments to the Maryland Department of Information Technology ("DoIT") Office of Security Management and the Maryland Department of Emergency Management.

Since enacted, the Commission, in coordination with the DoIT, has been working with the Cybersecurity Reporting Work Group, a group established by the Commission to enact regulations as required by House Bill 969. These efforts are ongoing, and utilities are expected to submit third-party assessment certifications in July 2024. Further, the Commission notified stakeholders of a rulemaking session scheduled for March 27th in response to the comments filed earlier in the month by several parties including, the Staff of the Public Service Commission (Staff), the Office of People's Counsel, Members and Staff

Charles Washington| Brittany Jones | Guy Andes| Dytonia Reed| 410.269.5281

of the Maryland Cybersecurity Council, the Joint Utilities[1], the American Gas Association (AGA), the Alliance for Digital Innovation, the Edison Electric Institute (EEI), and the Office of Senator Katie Fry Hester. The Commission should be allowed to continue on-going work. *House Bill 1420,* however, is duplicative of the Commission's current jurisdictional scope and is fiscally inefficient as well as overlaps current Commission led efforts.

Additionally, the legislation creates new definitions for *"zero-trust", "critical software*" and it expands other terms from House Bill 969. BGE supports aligning the definitions and standards with an existing cybersecurity framework (NIST-CSF). Furthermore, the definitions and standards should not be 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.

Lastly, there is a need to ensure that information about security and sensitive critical infrastructure operations be shared thoughtfully to maintain the chain of custody for that information from potential threat actors.

We strongly urge the General Assembly to reconsider legislation that creates overlapping regulatory obligations and to prioritize regulatory harmonization and fiscal responsibility.

For these reasons, BGE requests an unfavorable report on *House Bill 1420*.

[1] The Joint Utilities are collectively Baltimore Gas and Electric Company, Chesapeake Utilities Corporation, Delmarva Power & Light Company, Potomac Edison Company, Potomac Electric Power Company, Southern Maryland Electric Cooperative, Choptank Electric Cooperative, Inc., Columbia Gas of Maryland, Inc. and Washington Gas Light Company

Charles Washington| Brittany Jones | Guy Andes| Dytonia Reed| 410.269.5281

HB1420_Unfavorable_PSC.pdf
Uploaded by: Frederick Hoover
Position: UNF

STATE OF MARYLAND

PUBLIC SERVICE COMMISSION

March 27, 2024

Chair Brian J. Feldman
Education, Energy, and the Environment Committee
2 West, Miller Senate Office Building
Annapolis, MD 21401

RE: HB 1420 – Unfavorable –- Cybersecurity – Office of People's Counsel, Public Service Companies, Public Service Commission, and Maryland Cybersecurity Council

Dear Chair Feldman and Committee Members:

During the 2023 Session, the Maryland General Assembly enacted House Bill 969 (HB0969) entitled, "Public Service Commission – Cybersecurity Staffing and Assessments (i.e., the "Critical Infrastructure Cybersecurity Act of 2023" or "the Act").[1] As introduced, the Act was focused on requiring public service companies to implement certain cybersecurity standards, conduct independent third-party cybersecurity assessments every two years and report cybersecurity incidents to the Maryland Department of Information Technology (DoIT) Office of Security Management, among other things. HB0969 was codified in Public Utilities Article (PUA), § 2-108 and §5-306, Annotated Code of Maryland, which was enacted July 1, 2023. The Commission has a rulemaking session scheduled March 27, 2024, to codify these statute requirements in COMAR.

HB 1420 introduces definitions currently not codified in PUA § 5-306 for critical software and supply chain risk. HB 1420 then requires an assessment of critical software when public service companies engage with a third party to conduct an assessment of their cybersecurity standards adherence every two years as currently required by PUA § 5-306. HB 1420 also requires that public service companies establish minimum standards for supply chain risks. Finally, HB 1420 defines cyber resilience and requires that cyber resilience be added to service quality and reliability standards in PUA § 7-213. HB 1420 also adds a definition for critical infrastructure but does not have any direct requirements in the bill related to this definition.

Without commenting on OPC's needs to participate in cybersecurity matters associated with the Commission's implementation of PUA § 5-306 changes established in CY2023, other aspects of the bill are either redundant with existing PUA § 5-306 requirements, or are not needed.

The current definitions of operational technology and information technology systems, in COMAR 20.06 are already included in the scope of third-party assessments of public service company standards

[1] Delegate Qi sponsored HB 969. Senator Hester introduced the identical cross-file to HB0969 as Senate Bill 800.

adherence every two years. Operational technology and information technology system assessments include software. Therefore HB 1420's requirements for critical software are not needed.

Furthermore, supply chain risk does not need to be given additional emphasis in HB 1420 since PUA § 5-306(c)(3) already requires the establishment of minimum-security standards for supply chain risks.

In addition, the addition of cyber resilience in PUA § 7-213 is misplaced as this section of the Maryland Annotated Code is primarily related to electric utility reliability, not cybersecurity. Codification of cyber resilience in a section of the Maryland Annotated Code related to electric utilities misses the fact that PUA § 5-306 cybersecurity requirements are applicable to all public service companies, including gas and water utilities. Therefore, this statute requirement would not apply to water and gas public service companies that are subject to PUA §5-306.

Finally, the addition of cyber resilience requirements is not needed because the utility periodic assessments required by PUA § 5-306 every two years already need to be performed using either the Cybersecurity and Infrastructure Security Agency's Cross-Sector Cybersecurity Performance Goals (CPG) or a more stringent standard that is based on the National Institute of Standards and Technology (NIST) security frameworks. Both the CPG and NIST frameworks for assessments include an evaluation of the ability of a public service company to identify, protect, detect, respond, and recover from cyber-attacks, which is synonymous with the intent of the HB 1420 definition for cyber resilience[2]. Therefore, the cyber resilience requirement in HB 1420 is not needed.

I appreciate the opportunity to provide unfavorable testimony on HB 1420. Please contact the Commission's Director of Legislative Affairs, Christina M. Ochoa, at christina.ochoa1@maryland.gov if you have any questions.

Sincerely,

Frederick H. Hoover, Chair
Maryland Public Service Commission

[2] In HB 1420, "Cyber resilience" means the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

2024- PHI- HB1420- UNF.pdf
Uploaded by: Katie Lanzarotto
Position: UNF

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

Senate Opposition Letter - HB1420.pdf
Uploaded by: Timothy Troxell
Position: UNF

PotomacEdison
A FirstEnergy Company

Timothy R. Troxell, CEcD
Senior Advisor, Government Affairs
301-830-0121
ttroxell@firstenergycorp.com

10802 Bower Avenue
Williamsport, MD 21795

OPPOSE – House Bill 1420
HB1420 – Cybersecurity – Office of People's Counsel, Public Service Companies, Public Service Commission, and Maryland Cybersecurity Council
Senate Education, Energy, and the Environment Committee
Tuesday, March 28, 2024

Potomac Edison, a subsidiary of FirstEnergy Corp., serves approximately 285,000 customers in all or parts of seven Maryland counties (Allegany, Carroll, Frederick, Garrett, Howard, Montgomery, and Washington). FirstEnergy is dedicated to safety, reliability, and operational excellence. Its ten electric distribution companies form one of the nation's largest investor-owned electric systems, serving customers in Ohio, Pennsylvania, New Jersey, New York, West Virginia, and Maryland.

Unfavorable

Potomac Edison / FirstEnergy opposes House Bill 1420 – *Cybersecurity – Office of People's Counsel, Public Service Companies, Public Service Commission, and Maryland Cybersecurity Council*. HB-1420 authorizes the Office of People's Counsel (OPC) to retain or hire experts in cybersecurity, requires public service companies to have a third-party assessment of critical software, and adds additional cybersecurity requirements.

Potomac Edison / FirstEnergy requests an Unfavorable report on HB-1420. Adding additional requirements to the *Critical Infrastructure Cybersecurity Act of 2023*, while it is still evolving, will lead to additional costs and time delays in implementation.

Codifying detailed cybersecurity rules in legislation, which by nature evolves slowly, creates problems in the fast-moving landscape of technology and cybersecurity. Potomac Edison / FirstEnergy 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 for our customers. From a practical security perspective, additions proposed in HB-1420 would not materially improve upon what Maryland's investor-owned utilities are already doing in the cybersecurity arena under the supervision of the Maryland Public Service Commission (PSC). This legislation could result in significant additional costs for Maryland citizens and create regulatory confusion for the public service companies.

Boundaries between the PSC and the Maryland Department of Information Technology have been problematic in the implementation of the *Critical Infrastructure Cybersecurity Act of 2023*. The PSC's Cybersecurity Working Group is currently struggling to determine and obtain consensus on the requirements and meaning of last sessions legislation. Adding OPC, and new or changed definitions related to Zero Trust, Supply Chain Risks, and other key terms, would only compound the problems. Attempts to codify "Cyber Resilience" as some form of operational metric or standard is likely impossible, as no such uniform concept exists. In addition, the inclusion of "Critical Software" and the requirements for analyzing it are not risk-informed and are incompatible with the nature of software technology. The legal requirement to analyze such software would be nearly impossible for a public service company to comply with, as we generally cannot have access to the source code of commercial software. Even if it were possible to perform the analysis, the cost to analyze every item that could be included in the overly broad definition of "Critical Software" would be incredibly expensive

and labor exhaustive. Making all these changes in the middle of the PSC's Rulemaking Process would force a reset, leading to even more delay before any meaningful security changes come to fruition.

Potomac Edison / FirstEnergy manages cybersecurity costs, and performance is enhanced, by managing the corporation's entire multi-utility system on a central and uniform basis. We constantly are improving our cybersecurity programs to stay ahead of threats. Divergence from federal and national norms for cybersecurity regulations and creating very specialized requirements in law may introduce unintended risks to the consistent and successful compliance programs we and the other Maryland utilities currently maintain.

We believe this legislation will result in current cybersecurity processes becoming extremely burdensome and expensive, without creating any benefit to Maryland customers. For these reasons, **Potomac Edison / FirstEnergy respectfully request an <u>Unfavorable</u> report on HB-1420.**

HB1420 in the Senate OPC Testimony.pdf
Uploaded by: David Lapp
Position: INFO

DAVID S. LAPP
PEOPLE'S COUNSEL

WILLIAM F. FIELDS
DEPUTY PEOPLE'S COUNSEL

JULIANA BELL
DEPUTY PEOPLE'S COUNSEL

OPC
OFFICE OF PEOPLE'S COUNSEL
State of Maryland

6 ST. PAUL STREET, SUITE 2102
BALTIMORE, MARYLAND 21202
WWW.OPC.MARYLAND.GOV

BRANDI NIELAND
DIRECTOR, CONSUMER
ASSISTANCE UNIT

CARISSA RALBOVSKY
CHIEF OPERATING OFFICER

BILL NO.:	House Bill 1420 – Cybersecurity – Office of People's Counsel, Public Service Companies, Public Service Commission, and Maryland Cybersecurity Council
COMMITTEE:	Education, Energy, and the Environment Committee
HEARING DATE:	March 28, 2024
SPONSOR:	Delegate Kaiser
POSITION:	Informational

****

The Office of People's Counsel offers the following information on House Bill 1420. As introduced, HB 1420 would have required OPC to hire at least one Assistant People's Counsel with cybersecurity expertise to monitor utility compliance with cybersecurity standards and support utilities in remediating vulnerabilities or addressing cybersecurity assessment findings, among other duties.

The amendments adopted in the House appropriately clarify that OPC is not responsible for oversight of the cybersecurity practices of public service companies and eliminates the requirement that OPC hire at least one Assistant People's Counsel with cybersecurity experience. Instead, the bill would add "cybersecurity" to the list of fields for which OPC may hire outside experts. Although OPC has in the past engaged experts in cybersecurity under the existing general authority to hire experts in "utility regulation," OPC does not object to the more specific grant of authority provided for in HB 1420, as amended by the House.