SUPPORT WITH AMENDMENT

John M. Abeles
President and CEO of System 1, Inc.
a cybersecurity and Critical Infrastructure Consultancy

Testimony in Support of

HB 969, **"**Public Service Commission – Cybersecurity Staffing and Assessments (Critical Infrastructure Cybersecurity Act of 2023)**"**
Sponsor: Delegate Lily Qi

House Economic Matters Committee, 1 p.m. March 9, 2023

Honorable Chair and members of the committee, thank you for the opportunity to provide testimony in support of Senate Bill 969 pertaining to cybersecurity and the Maryland Public Service Commission ("PSC").

My name is John M. Abeles. I have over 30 years supporting the Energy Sector and serve as a member of the Maryland Cybersecurity Council. I have supported and led efforts in critical infrastructure protection, risk management, and cybersecurity for the White House; Departments of Energy, Commerce, Interior, and Treasury; some private sector utilities; and states.

Context – Maryland needs to build a resilient approach to cybersecurity and needs to foster an agile culture to counter the evolving threat and vulnerability landscape. Under House Bill 969, the PSC is the organization responsible for establishing the aiming points and for monitoring how utilities are meeting these requirements.

A GAO report[1] for Congress in August 2019, on "Critical Infrastructure Protection on Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid," highlighted that the threat environment has increased from hostile nations, criminal groups, terrorists; and others are increasingly capable of attacking the grid. The cyber systems in Maryland have vulnerabilities, including those that involve industrial control systems that support grid operations. While large scale impacts on the grid have not yet been realized, the report indicates that federal assessments indicate that cyberattacks could cause widespread power outages in the United States.

In addition, industry and the Government have noted the importance of improving their cybersecurity posture. A Price Waterhouse Cooper (PWC) document[2] from the 2023 Global Digital Trust Insights shows that senior executives worry that their enterprise isn't fully prepared to address heightened threats. Topping the 2023 list of rising organizational threats are cybercriminal activity (65%); mobile devices (41%), emails (40%), cloud-based breaches (38%); and business email compromise/account takeovers (33%) and ransomware (32%). Forty-two

[1] https://www.gao.gov/products/gao-19-332

[2] A C-suite united on cyber-ready futures: PwC

percent of senior executives say cyber breaches of their systems have increased since 2020. These apply to a broad range of industries including energy generation and distribution.

Support for the Bill – House Bill 969 has a number of essential provisions that requires only minimal cost and employee resources, and can be scaled based the size and complexity of the utility. The bill needs to counter the expanding threat and evolving vulnerability landscape.

The bill has a provision for assuring one or more of the PSC's employees are experts in cybersecurity to advise the Commissioners, ensure that there is sufficient funding, consult with the Maryland Office of Security Management, study cybersecurity best practices, assist in drafting cybersecurity regulation, provide oversight of public service practices, and assist the PSC in monitoring public service company's security standards. Agility is required as many of the nation-wide cybersecurity regulations and guidance are currently being enhanced. The National Cybersecurity Strategy[3] was issued by the White House on March 2, 2023. The strategy seeks to build and enhance collaboration around five pillars, the first of which is to defend critical infrastructure. This will include the expansion of minimum cybersecurity requirements, harmonize regulations to reduce the burden of compliance, and enable public-private partnerships. Three recent examples of cybersecurity regulations and guidance that are enhanced include:

- Nuclear Regulatory Commission Regulatory Guide 5.71, revision 1, Cybersecurity Program for Nuclear Power Reactor, issued February 2023[4]
- Department of Energy, Cybersecurity Capability Maturity Model, Version 2.1, issued in June 2022[5]
- National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0, Is in the process of development and public comments. Last meeting February 2023[6]

During the Winter Meeting of the National Association of Regulatory Utility Commissioners (NARUC) in Washington, DC, in February 2023, CISA reminded the audience that minimizing physical and cybersecurity is a priority for state regulators and utilities and that information sharing was key to developing a proactive security posture, improve on developing and mitigating security challenges both for utilities and regulators, and improving response and recovery efforts to security events through effective private and public relationships.

As an amendment to HB 969, at least one of the experts should be required to have (or obtain) a Top Secret or Q clearance, so that that sensitive information and responses can be shared with state personnel. The added expertise, missing from current Commission staffing, is needed to provide adequate understanding of the challenges and appropriate actions necessary to defend Maryland utilities from cyber-attack or inadequate cyber planning.

---

[3] https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

[4] https://www.govinfo.gov/content/pkg/FR-2023-02-13/pdf/2023-02941.pdf

[5] https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf

[6] https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20

In addition, the bill parallels many of the Federal and industry requirements and guidance but will focus on those items at the state level.

Specific issues -- The bill has provisions to establish and share cybersecurity standards and best practices, and prepare an evaluation of utilities cybersecurity policies, procedures, and expertise. It also requires the development of formal reports on cybersecurity threats and sources and the efficacy of protective cybersecurity practices. To date no formal or written report has been prepared or made available to key Maryland departments (even on a confidential basis). Only a quick verbal presentation is made to Commissioners with no written documentation provided for further review. Currently there is no assurance that weaknesses identified during the briefings are documented or later mitigated. Having documentation would provide a basis to judge the ongoing adequacy of a utility's cybersecurity program. Understanding the sensitivity of vulnerability and weakness information of specific corporate entities might hinder the open reporting of information to the PSC. To counter this issue, as a second amendment, the information could be identified as Critical Energy Infrastructure Information[7] (CEII). This is a class of information that is sensitive and is exempt from disclosure through the Freedom of Information Act (FOIA) and other public disclosure requests. I support amending the bill to include the use of CEII.

The bill is predicated on a zero-trust approach. That requires all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. Zero Trust is a framework for securing infrastructure and data for today's modern digital transformation. It uniquely addresses the modern challenges of today's business, including securing remote workers, hybrid cloud environments, and ransomware threats.

The bill also requires the identification of security risks associated with supply chains and a bi-annual third-party review in concert with NIST's security frameworks that will be submitted to the PSC.

Path Forward -- House Bill 969 with suggested amendments provides a path forward to protect Maryland's critical energy infrastructure. Further enabling the PSC's function by adding expertise and formality to their processes will advance a culture of continuous improvement. The added funding and resources will allow agility to progressively update and keep pace with the evolving challenges that Maryland utilities will encounter.

[7] https://www.ecfr.gov/current/title-18/chapter-I/subchapter-X/part-388/section-388.113