TESTIMONY PRESENTED TO THE
HOUSE ECONOMIC MATTERS COMMITTEE

HB 1339
CYBERSECURITY - CRITICAL INFRASTRUCTURE AND PUBLIC SERVICE COMPANIES (CRITICAL INFRASTRUCTURE SECURITY ACT OF 2022)

DR. GREG VON LEHMEN
UNIVERSITY OF MARYLAND GLOBAL CAMPUS
STAFF TO THE MARYLAND CYBERSECURITY COUNCIL
POSITION: SUPPORT WITH AMENDMENTS

MARCH 3, 2022

Chairman Wilson, Vice Chairman Crosby, and Members of this Committee, thank you for the opportunity to submit testimony in support of HB 1339.

I am Dr. Greg von Lehmen, University of Maryland Global Campus, and staff to the Maryland Cybersecurity Council. I am providing testimony solely in my role as staff to the Maryland Cybersecurity Council. I support HB 1339 with amendments.

The bill comes at a time of urgency with respect to threats to the nation's and State's critical infrastructure, including companies covered by the bill. These threats have been well documented by the US Department of Homeland Security Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation, and the National Security Agency, among others.

The bill answers this urgency by including well-grounded provisions that would assist the Public Service Commission and covered public service companies address this accelerating risk. Specifically, the bill is informed by an extensive year-in-the-making report published in December by the Maryland Cybersecurity Council. The report was prepared for the Council by an employee of the NSA who worked full time for twelve months in the Attorney General's Office under a fellowship arrangement with that agency.

The report is based on State and federal legal research, interviews with the State officials, officials in other states, and a number of subject matter experts, including a former executive of the North American Electric Reliability Corporation (NERC). The bill reflects various recommendations of the report in its requirements concerning zero trust and resiliency, the inclusion of a cybersecurity expert on the staff of the Public Service Commission, ensuring cybersecurity risk is an explicit factor in the Commission's rulemaking, and standards that covered public service companies should implement, among others.

The most significant amendments that I recommend are to a) specify recognized cybersecurity standards that covered public service companies could choose from in order to meet the requirements of the bill, and b) permit the Public Service Commission the leeway to gauge

reasonable compliance with the selected standard(s) by considering a variety of factors, such the size, complexity, and resources of the covered public service companies in view. These amendments would provide these companies with clarity about the standards to be implemented and should preclude demands for levels of effort that are reasonably beyond a company's capacity. At the same time, the specificity of the standards provides an assurance to the State and its citizens that appropriate efforts are being made to reduce cybersecurity risk.

As key federal agencies advise all of us, this is time of elevated risk to our public service companies and our critical infrastructure in general. HB 1339 answers these advisories. I support the bill with amendments and urge a favorable report by the committee.

Thank you.