

TESTIMONY PRESENTED TO THE
SENATE FINANCE COMMITTEESB 691
CYBERSECURITY - HEALTHCARE ECOSYSTEMDR. GREG VON LEHMEN
February 27, 2025

Madam Chair, Mr. Vice Chair, and members of the committee, good afternoon and thank you for the opportunity to testify in favor of SB 691. I am Dr. Greg von Lehmen, special assistant for cybersecurity at UMGC and staff to the Maryland Cybersecurity Council. My comments today in support of the bill are my own and are not intended to represent the views of these organizations.

Given the testimony today, I would say the question is not so much whether to act but what action to take. This question will become more urgent as new technologies, like AI, are increasingly incorporated into the attacker toolbox, reducing attacker costs and turbocharging the scale and effectiveness of attacks.¹

The bill has two significant virtues.

First, it recognizes the complexity of the problem and puts in place a deliberate process to address it. Healthcare cybersecurity of course starts with the cybersecurity of the individual members. The bill has provisions that aim to enhance the general security posture of the individual ecosystem members. That is foundational. It helps mitigate the problem.

But it is not enough. Addressing the vulnerability that stems from the interconnectedness of the ecosystem is critical. Representatives of all entities involved have to be brought together to identify what especially needs to be protected and to work out the business continuity arrangements *between* the ecosystem members to provide essential patient services in an emergency.

The bill recognizes this need for such a convening by providing for it by design. Not as a one-time event but as an ongoing practice to pace with the threat while

¹ See for example, Heikkeliä, M (2024, May 21). [Five ways criminals are using AI](#) MIT Technology Review, and MIT Technology Review Insights (2021). [Preparing for AI-enabled cyberattacks](#).

including the relevant State government agencies and departments with their particular roles and strengths.

Second, the fact that SB 691 would use a tried and true regulatory model to address the cybersecurity of its healthcare sector is a significant benefit. If you subtract out from the bill the provisions that are particular to the subject matter—the definitions of the healthcare ecosystem, “essential capabilities”, MHCC and MIA as the agencies involved, and so forth—what you are left with is Maryland’s Critical Infrastructure Act of 2023 that concerned the PSC and utilities serving Maryland. The provisions pertaining to cybersecurity requirements, the staffing support for the agencies, and the various processes described in SB 691 are all carried over from that Critical Infrastructure Act.

What is the benefit of this? I served both on the workgroup that helped inform the 2023 statute and also participated in the cybersecurity working group that the PSC convened to inform its rulemaking under the statute. I would very much expect that lessons learned from that process would be of value to the agencies and the stakeholders involved in the implementation of SB 691.

Like electricity, healthcare is critical to Maryland residents. The General Assembly has acted with respect to the former. It should now address the latter. I urge a favorable report.

Thank you.