

TESTIMONY PRESENTED TO THE
SENATE EDUCATION, HEALTH AND ENVIRONMENTAL AFFAIRS COMMITTEE

SENATE BILLS 780 (CYBERSECURITY GOVERNANCE ACT OF 2022) AND SB 812
(CYBERSECURITY – COORDINATION AND GOVERNANCE)

DR. GREG VON LEHMEN
UNIVERSITY OF MARYLAND GLOBAL CAMPUS
MEMBER AD HOC COMMITTEE ON STATE AND LOCAL CYBERSECURITY
POSITION: SUPPORT

MARCH 3, 2022

Chairman Pinsky, Vice Chairwoman Kagan, and Members of this Committee, thank you for the opportunity to submit testimony in support of SB 780 and SB 812.

I am Dr. Greg von Lehmen, University of Maryland Global Campus and staff to the Maryland Cybersecurity Council. I am providing testimony as a member of the Council's Ad Hoc Committee on State and Local Cybersecurity whose [report](#) was published in January.

I urge the Committee to support both SB 780 and SB 812 in a unified version for the following reasons.

First, the consolidation of responsibility for cybersecurity and IT that these bills propose would address challenges that DoIT faces in providing cybersecurity for the State Executive Branch. These challenges include a lack of visibility into systems and applications used by departments, compliance with the State Security Manual, their cybersecurity budgets, staffing, and security priorities, among other things. What cannot be seen cannot be secured. Unifying responsibility for cybersecurity in DoIT would reduce these challenges.

Second, the consolidation of cybersecurity and IT responsibilities in DoIT would enable the State to reap not only greater security but to see more clearly where economies of scale and lower costs for IT and security applications, systems, and services can be attained by implementing common systems across Executive Branch departments.

Third, this consolidation would allow departments and agencies to focus on why they were created—their business or service mission—rather than requiring them to split management and staff time and attention on maintaining and securing their IT infrastructure.

Finally, in implementing a consolidated model, DoIT would have several advantages. It has an extensive amount of survey data that was collected from the departments as part of the ad hoc study to help it establish priorities. It will have an enhanced governance group, the Maryland Cyber Coordinating Council, a representative body of Executive Branch department heads, to provide advice and counsel. Importantly, it has the experience of other states to learn from. As examples, both Vermont and North Dakota have centralized the provision of their IT and

cybersecurity and provided testimony last year to the Joint Committee on IT, Cybersecurity and Biotechnology regarding the benefits that they have experienced.¹

The purpose of the Ad Hoc Committee study was to take an objective look at the challenges faced by DoIT in serving the Executive Branch. The committee included CHHS, MDEM, DoIT, and MACo. Its work was supported by testimony from many other groups last year before the Joint Committee on IT, Cybersecurity, and Biotechnology. An effort was made to learn as much as possible from states, with interviews conducted outside of the hearings with CISOs and CIOs in New Hampshire, New Jersey, and North Dakota. The National Governor's Association, the National Association of State CIOs, and the nonprofit Center for Internet Security, among others, were all consulted. Such a study presents the State with a unique opportunity to move forward in an informed way.

For the good of Maryland, I urge the committee to support a consolidated version of SB 780 and SB 812.

Thank you.

¹See testimony provided to the Joint Committee by Mr. John Quinn (State of Vermont CIO) on June 23, 2021 and by Mr. Shawn Riley (State of North Dakota CIO) on September 29, 2021, at https://mgaleg.maryland.gov/mgawebsite/Committees/Media/false?cmte=mjm&clip=MJM_6_23_2021_meeting_1&ys=2021rs, https://mgaleg.maryland.gov/mgawebsite/Committees/Media/false?cmte=mjm&clip=MJM_9_29_2021_meeting_1&ys=2021rs