Maryland
DEPARTMENT OF INFORMATION TECHNOLOGY

Wes Moore | Governor
Aruna Miller | Lt. Governor
Katie Savage | Secretary

TO: Senate Education, Energy, and the Environment Committee
FROM: Department of Information Technology
RE: Senate Bill 691- Cybersecurity - Healthcare Ecosystem
DATE: February 27, 2025
POSITION: Letter of Information

The Honorable Pamela Beidle
Senate Finance Committee
3 East Miller Senate Office Building
Annapolis, Maryland 21401

Dear Chairwoman Beidle,

The Department of Information Technology (DoIT) appreciates the opportunity to provide information regarding Senate Bill 691- Cybersecurity - Healthcare Ecosystem, which aims to enhance cybersecurity measures across Maryland's healthcare ecosystem. We recognize the importance of improving cybersecurity resilience and ensuring the protection of sensitive healthcare data. After reviewing the bill's provisions, we would like to offer insights and considerations for committee members.

SB 691 appropriately emphasizes the need for adopting Zero-Trust (ZT) principles, which align with industry best practices. However, it is critical to recognize that ZT is not an immediate solution but a long-term framework requiring incremental implementation. Rushing ZT adoption may inadvertently introduce vulnerabilities rather than strengthening cybersecurity. We recommend that the bill require a structured implementation plan with key milestones, incorporating tailored audits at each stage to assess the evolving security posture.

The bill's reporting requirements present an opportunity to enhance Maryland's cybersecurity intelligence. Presently, the Office of Security Management (OSM) has limited ability to derive actionable insights from such reports. To maximize the value of this data, we suggest incorporating language that suggests consulting with the Chief Data Officer when developing a centralized repository for cybersecurity reports. This would ensure data is utilized effectively for improved threat detection and response.

The bill's reporting requirements closely align with the Critical Infrastructure Cybersecurity Act of 2023. However, challenges arose with that legislation, as utility companies successfully

contested OSM's minimum reporting standards before the Public Service Commission (PSC). To avoid similar obstacles, HB 333 should explicitly affirm the authority of the State Chief Information Security Officer (SCISO) in defining and enforcing reporting standards upon publication. Alternatively, resolving prior challenges with the PSC before implementation could provide a more stable foundation for enforcing cybersecurity regulations.

SB 691 assigns the Maryland Department of Emergency Management (MDEM) a role in providing guidance on cybersecurity regulatory standards for healthcare ecosystem entities. However, governance, risk, and compliance (GRC) functions typically fall within the purview of regulatory and cybersecurity agencies such as DoIT. We recommend revising this provision to ensure regulatory oversight aligns with the appropriate agency's expertise.

The bill references multiple cybersecurity frameworks, including NIST 800-207, NIST 800-207A, NIST 800-53A, the NIST Cybersecurity Framework, and the Health Industry Cybersecurity Practices (HICP). While each framework offers valuable guidance, inconsistencies may arise if different healthcare entities adopt conflicting standards. A clearer approach may be to align the bill's requirements with a single overarching cybersecurity framework, such as the NIST Cybersecurity Framework or the Cybersecurity and Infrastructure Security Agency's (CISA) Cyber Performance Goals (CPGs), to ensure uniformity across the ecosystem.

The Department of Information Technology supports the overarching goals of SB 691 and its intent to strengthen cybersecurity protections within Maryland's healthcare ecosystem. We believe that refining the bill's approach to Zero-Trust implementation, aggregate reporting, MD-SOC authority, regulatory oversight, and cybersecurity framework alignment will enhance its effectiveness and ensure its successful implementation. We appreciate the opportunity to provide these insights and welcome further discussion on these critical cybersecurity matters.

Best,

Melissa Leaman
Acting Secretary
Department of Information Technology