



**Mohammed Choudhury**  
State Superintendent of Schools

---

<b>BILL:</b>	SB780	<b>DATE:</b>	March 3, 2022
<b>SUBJECT:</b>	Cybersecurity Governance Act of 2022	<b>COMMITTEE:</b>	Education, Health, and Environmental Affairs
<b>POSITION:</b>	Support with Amendments		
<b>CONTACT:</b>	Ary Amerikaner 410-767-0090 <a href="mailto:ary.amerikaner@maryland.gov">ary.amerikaner@maryland.gov</a>		

The Maryland State Department of Education (MSDE) supports with amendments **Senate Bill 780 – Cybersecurity Governance Act of 2022**, which would establish the Office of Security Management within the Department of Information Technology (DoIT), names the head of the new office as the State Chief Information Security Officer (SCISO), creates Directors of Local and State Cybersecurity, establishes the Maryland Cybersecurity Coordinating Council, and amends the definitions of cybersecurity and information technology.

As a custodian of sensitive data for over 900,000 Maryland public school students and thousands of public-school staff, protecting this information is a top priority. MSDE supports strong security protocols. We are fully committed to the cybersecurity goals of the state and support the relevant measures proposed in the legislation. As a DoIT enterprise agency, MSDE staff works with the State Chief Information Security Officers’ team regularly. MSDE receives monthly reports from DoIT identifying any vulnerabilities to applications on MSDE’s network. MSDE’s Information System Security Officer works with stakeholders to mitigate the identified vulnerabilities. MSDE has also worked with DoIT in transitioning identified obsolete IT infrastructure (servers, systems etc.) to a supported platform. At present, MSDE and DoIT are jointly working on a series of cybersecurity assessments to understand the maturity of our data management programs, our security posture, data governance, and security configurations. In addition, MSDE IT leadership has been directed to ensure that security trainings released by DoIT are completed by all staff as they are released. MSDE currently has a contractual security professional from an approved DoIT vendor assigned as Information System Security Officer (ISSO). MSDE is working on establishing a fulltime position, Chief Information Security Officer (CISO), to oversee this work and increase collaboration and coordination with the current and new security processes, protocols and personnel established by DoIT.

**However, MSDE has serious concerns that the part of the bill that shifts control of all IT functions to another agency will have an adverse impact on the operations of the Department, undermining our ability to ensure high quality IT support for our employees and constituents.** This can be loosely grouped into three related concerns:

1. **Mission aligned support that meets agency timelines and quality standards.** An organization’s technology operations go beyond the secure networks and standardized software systems that support operations. It requires IT staff that understands the priorities of the agency

and works to put them in the forefront. The IT staff needs to be keenly aware of the program priorities, laws, regulations and deadlines that drive the work. It is important that they report to the head of the agency who can ultimately ensure that program priorities and customer service expectations are reflected in the IT team's work product.

As part of the new administration's first phase of reorganization, we have utilized existing vacancies in the department to create IT partner positions and structured them to work with their counterparts in other parts of the agency to provide a high quality and continuous customer service to the divisions. Absorbing these newly created positions into DoIT and associated transition will cause disruption and will have negative impact on MSDE's ability to create a high functioning department as we implement the Blueprint for Maryland's Future. Therefore, the language in the bill that broadly defines anyone working more than 50% of their time on IT operations as becoming DoIT employees is concerning.

2. **Specialized knowledge of the field.** The information technology service needs of MSDE range from supporting technology needs of the regional offices in the Division of Early Childhood to supporting high quality data analysis and reporting in research and assessment offices. These needs cannot be effectively met by a centralized operation that is designed to meet the overall needs of many agencies. In one recent example, MSDE submitted an RFP to start a College and Career Ready study. This subject matter is entirely outside of DoIT's core area of work, and yet they must review it, which results in significant involvement from MSDE staff to provide subject matter guidance.
3. **Procedural bottlenecks and timeline delays.** Too often, the structure of a centralized IT support program leads to consistent delays and bottlenecks for agencies. For example, MSDE currently submits all technology procurement requests to the DoIT intake committee for review and approval prior to purchase. When software as a service (SaaS) products are procured, MSDE must submit system control documentation and system security plans prior to receiving an authority to operate from DoIT. As MSDE is one of many customers serviced by DoIT, we have experienced delays in getting the reviews expeditiously. We recently have experienced several week delays in, for example, (a) obtaining a resource for urgently needed website updates and (b) reviewing a high priority Blueprint for Maryland's Future Request for Proposals (RFP).

While IT staff employed by our department have worked through these limitations to ensure the needs of the department are met, this experience reinforces the MSDE belief that IT staff employed by the agency are critical to our success.

MSDE's experiences and concerns above are not a reflection on the commitment and skills of the DoIT leadership or staff. Instead, they reflect (1) a lack of standardized collaboration norms and service expectations across multiple agencies; (2) an inadequate level of staffing at DoIT to fulfill obligations to their customers; and (3) the impossible task of knowing enough about multiple state agencies' complicated work to meaningfully support their IT needs.

Absorbing the IT operations of the department into DoIT will only exacerbate the challenges outlined above and cause unaccounted disruptions due to transition. This is especially concerning to MSDE as we accelerate into the first few years of meaningful implementation of the Blueprint for Maryland's Future.

MSDE proposes a collaborative approach to mitigate these concerns. This would include amendments that:

- Allow MSDE to retain ownership of existing IT resources;
- Establish regular communication channels between DoIT and the department stakeholders;
- Establish IT hiring standards across all agencies that align with the overall cybersecurity objectives of the state;
- Establish standard evaluation protocols that ensure effective evaluation of the IT resources that align with the security regulations;
- Require IT staff at the agencies complete mandatory minimum trainings each year to stay updated on the latest skill levels required to operate and support mission critical enterprise systems;
- Increase internal and external penetration testing and security analysis;
- Include MSDE personnel as part of the DoIT procurement intake processes related to MSDE IT needs to establish joint ownership of the processes and planning; and
- Explore procurement process efficiencies to reduce the time taken to complete the procurement process

We respectfully request that you consider this information as you deliberate Senate bill 780. Please contact Ary Amerikaner, at 410-767-0090, or [ary.amerikaner@maryland.gov](mailto:ary.amerikaner@maryland.gov), for any additional information.