Department of Legislative Services

Maryland General Assembly
2024 Session

FISCAL AND POLICY NOTE
First Reader

Senate Bill 981 (Senator Hester)

Education, Energy, and the Environment and Budget and Taxation

Local Cybersecurity Preparedness and Local Cybersecurity Support Fund - Alterations

This bill (2) authorizes the Governor to include in the annual budget bill for fiscal 2026 and 2027 an appropriation of $10.0 million to the Local Cybersecurity Support Fund, and (2) requires the Department of Information Technology (DoIT) to provide sufficient information security officers to assist the Director of Local Cybersecurity in the execution of the director's duties. By July 1, 2025, a local school system must implement specified cybersecurity measures, and each year, a local school system must report in a cybersecurity assessment the percentage of employees that comply with the cybersecurity measures. The bill authorizes, for fiscal 2026 and 2027, funds from the Dedicated Purpose Account (DPA) to be transferred to implement the bill's requirements. **The bill takes effect July 1, 2024.**

Fiscal Summary

State Effect: Special fund expenditures from DPA increase by $10.0 million in FY 2026 and 2027. Special fund revenues and expenditures for the Local Cybersecurity Support Fund increase correspondingly as the funds are received and used for authorized purposes.

($ in millions)	FY 2025	FY 2026	FY 2027	FY 2028	FY 2029
SF Revenue	$0	$10.0	$10.0	$0	$0
SF Expenditure	$0	$20.0	$20.0	$0	$0
Net Effect	$0.0	($10.0)	($10.0)	$0.0	$0.0

Note:() = decrease; GF = general funds; FF = federal funds; SF = special funds; - = indeterminate increase; (-) = indeterminate decrease

Local Effect: Expenditures for local school systems may increase meaningfully, as discussed below. Revenues for local school systems increase to the extent that local governments apply for and receive funding from the Local Cybersecurity Support Fund. **This bill imposes a mandate on a unit of local government.**

Small Business Effect: Minimal or none.

Analysis

Bill Summary: By July 1, 2025, a local school system must implement (1) multifactor authentication for all school employees; (2) endpoint detection and response on all system-owned devices accessed by employees; and (3) network monitoring. Each year, a local school system must report in a cybersecurity assessment required by current law the percentage of employees that comply with these requirements.

Current Law: Chapters 241, 242, and 243 of 2022 expanded and enhanced the State's regulatory framework for State and local government cybersecurity. Among other things, the Acts required additional funding for cybersecurity, established leadership positions in State government for cybersecurity, codified existing cybersecurity requirements from a previous executive order, and required State and local governments to perform cybersecurity preparedness assessments.

The Acts also created the Local Cybersecurity Support Fund as a special, nonlapsing fund administered by the Secretary of Emergency Management. Its purpose is to provide financial assistance to local governments to improve cybersecurity preparedness and assist local governments applying for federal cybersecurity preparedness grants. The fund may be used only (1) to provide financial assistance to local governments to improve cybersecurity preparedness, as specified; (2) to assist local governments applying for federal cybersecurity preparedness grants; and (3) for administrative expenses, as specified.

Expenditures from the fund may only be made in accordance with the State budget. To be eligible to receive assistance from the fund, a local government must (1) provide proof to DoIT that the local government conducted a cybersecurity preparedness assessment in the previous 12 months or (2) within 12 months, undergo a cybersecurity preparedness assessment, as specified.

The Acts also required the Governor to include in the annual budget bill for fiscal 2024 an appropriation of at least 20% of the aggregated amount appropriated for information technology and cybersecurity resources in the annual budget bill for fiscal 2023. The fiscal 2024 budget as passed by the General Assembly included $152.0 million for the DPA, which is one of four accounts that make up the State Reserve Fund, to meet the mandated appropriations required for Chapters 241, 242, and 243. DoIT also processed a fiscal 2023 budget amendment to transfer $94.0 million from the DPA for remediation of State and local governments' cybersecurity.

State Fiscal Effect:

Local Cybersecurity Support Fund

The bill authorizes the Governor to include in the annual budget bill, for fiscal 2026 and 2027, an appropriation of $10.0 million to the Local Cybersecurity Support Fund, and authorizes funding from DPA to be used to fulfill the authorization.

Although funding is discretionary, this analysis assumes that funding in DPA originally allocated for cybersecurity purposes is used to provide the authorized funding. Thus, special fund expenditures from DPA increase by $10.0 million in fiscal 2026 and 2027, and special fund revenues for the Local Cybersecurity Support Fund increase correspondingly. Special fund expenditures from the Local Cybersecurity Support Fund increase correspondingly in fiscal 2026 and 2027 as the funding is used to support local cybersecurity related upgrades and activities, including staffing and equipment to comply with the bill's local mandate.

Department of Information Technology

The bill requires DoIT to provide sufficient information security officers to assist the Director of Local Cybersecurity in carrying out the director's duties. DoIT advises that it currently has three officers that work under the Director of Local Cybersecurity, which it characterizes as sufficient to fulfill the director's statutory duties. Therefore, DoIT does not require additional staff.

Local Fiscal Effect: Local school system expenditures may increase, potentially significantly, to meet the cybersecurity requirements required by the bill. Local school systems provided the following information regarding the bill's impact.

- Anne Arundel County Public Schools advises that it has already implemented multifactor authentication and endpoint monitoring for all employees; however, it anticipates a one-time cost of $200,000 and ongoing costs to hire a security engineer to implement the bill's network monitoring requirements;
- Prince George's County Public Schools anticipates additional costs of $400,000 annually to implement multi-factor authentication, a virtual private network, and additional network monitoring in order to meet the bill's requirements; and
- Montgomery County Public Schools and St. Mary's County Public Schools advise that they are already in compliance with the bill and, therefore, anticipate no fiscal impact.

Local revenues increase to the extent that local governments apply for and obtain grants from the Local Cybersecurity Support Fund. Assuming the transfer of funds from DPA to

the fund, grant funding is likely available in fiscal 2026 and 2027. However, local school systems may be responsible for any costs incurred in fiscal 2025 (since the bill requires the cybersecurity measures to be in place by July 1, 2025) and costs incurred beginning in fiscal 2028.

Additional Information

Recent Prior Introductions: Similar legislation has not been introduced within the last three years.

Designated Cross File: None.

Information Source(s): Department of Information Technology; Maryland Department of Emergency Management; Department of Budget and Management; Anne Arundel County Public Schools; Montgomery County Public Schools; Prince George's County Public Schools; St. Mary's County Public Schools; Department of Legislative Services

Fiscal Note History: First Reader - March 6, 2024
rh/mcr

Analysis by: Richard L. Duncan

Direct Inquiries to:
(410) 946-5510
(301) 970-5510