



Senator Brian Feldman, Chair  
Senator Cheryl Kagan, Vice-Chair  
Senate Education, Energy, and the Environment Committee  
Miller Senate Office Building, 2 West  
Annapolis, Maryland 21401

**Re: *Senate Bill 981: Local Cybersecurity Preparedness & Local Cybersecurity Support Fund – Favorable w/ Amendments***

**March 6, 2024**

Dear Chairman Feldman and Committee Members:

On behalf of Varonis Systems, I would like to take this opportunity to thank you for the opportunity to submit this letter of support with amendments to Senate Bill 981: *Local Cybersecurity Preparedness & Local Cybersecurity Support Fund*.

As written, Senate Bill 981 would authorize the Governor (in FY26 and FY27), to include in the annual budget bill an appropriation of \$10,000,000 for the Local Cybersecurity Support Fund. The Fund was established through the enactment of Chapter 241 - *Local Cybersecurity Support Act of 2022 (Senate Bill 754)*. The purpose of the Fund is to provide financial assistance to local governments to improve cybersecurity preparedness, including but not limited to network/device upgrades; recruitment; hardware/software support; training; and cybersecurity assessments.

Major data breaches from the past few years are reminders that cybersecurity can't remain an afterthought when it comes to budgeting priorities. The threat landscape is expanding and the likelihood of a cyber-attack is high. Luckily, more companies are taking their strategy seriously since investments in [cybersecurity budgets increased by 141 percent between 2010 and 2018](#).

In an article, titled "*The Future of Cybersecurity Budgeting*", Michael Buckbee stated, "companies are increasing their cybersecurity budgets". He further said, "the key to successfully using a cybersecurity budget relies on the relationship between top leadership and cybersecurity professionals. A company's overall security posture can improve if everyone is on the same page about budget allocations and how they impact the business." The same philosophy holds true for both state and local governments.

The investments made into strategic cybersecurity efforts towards increasing efficiency and decreasing response times will pay off for companies in the long run. With the recent recorded cyber attacks (and threats) to the State's departments and school systems, it is imperative for the State of Maryland to make these laudable investments now in order to avert future incidents.

In addition, Senate Bill 981 would require the Department of Information Technology (DoIT) to provide additional information security officers to assist (and support) the Director of Local Cybersecurity.

Finally, the bill would require that, by July 1, 2025, a local school system to implement for all school employees multifactor authentication, endpoint detection and response on all system-owned devices, and network monitoring. We believe this section of the bill could be strengthened to reflect the following friendly amendments:

*Amendment No.1* – Page 5, line 26: **STRIKE** the word “~~AND~~”.

*Amendment No.2* – Page 5, Line 27: **INSERT** the following, “**(3) DATA MONITORING DETECTION AND RESPONSE ON ALL SYSTEM DATA REPOSITORIES; AND**”

*Amendment No. 3* – Page 5, Line 27: **STRIKE** “(3)” and **INSERT** “(4)”.

It is for these reasons that Varonis supports the passage of Senate Bill 981, with the aforementioned amendments, and urges this committee to give this legislation a FAVORABLE report.

Thank you for your consideration and time.

Sincerely,



Jason Bonasera  
Varonis Systems, Inc.