

**Department of Legislative Services**  
 Maryland General Assembly  
 2023 Session

**FISCAL AND POLICY NOTE**  
**First Reader**

Senate Bill 868 (Senator Hester)  
 Education, Energy, and the Environment

**State and Local Cybersecurity - Revisions**

This bill makes various changes to the regulatory framework for State and local government cybersecurity established by Chapters 241, 242, and 243 of 2022. Among other things, the bill (1) requires the Governor, beginning in fiscal 2025, to include in the annual budget bill significant funding for cybersecurity in the Dedicated Purpose Account (DPA); (2) places the State Chief Information Security Officer (SCISO) under the supervision of the Governor instead of the Secretary of Information Technology; and (3) requires the Department of Information Technology (DoIT) to onboard agencies into its cybersecurity services under specified circumstances. **The bill takes effect June 1, 2023.**

**Fiscal Summary**

**State Effect:** General fund expenditures increase by \$1.0 million in FY 2023 and \$4.2 million in FY 2024 for reporting and staffing costs. Out-year general fund expenditures primarily reflect the mandated appropriation for DPA; special fund revenues for DPA increase correspondingly. Special fund expenditures are not *required* in any given year but may increase, as discussed below. Potential costs for DoIT staffing or to onboard affected State agencies into DoIT’s cybersecurity services have not been quantified, as discussed below. **This bill establishes a mandated appropriation and modifies an existing mandated appropriation beginning in FY 2025.**

(\$ in millions)	FY 2023	FY 2024	FY 2025	FY 2026	FY 2027
SF Revenue	\$0	\$0	\$173.6	\$208.4	\$250.0
GF Expenditure	\$1.0	\$4.2	\$173.8	\$208.5	\$250.2
SF Expenditure	\$0	\$0	-	-	-
Net Effect	(\$1.0)	(\$4.2)	(-)	(-)	(-)

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

**Local Effect:** The bill does not materially affect local government operations or finances.

**Small Business Effect:** Minimal.

## Analysis

**Bill Summary/Current Law:** Chapters 241, 242, and 243 expanded and enhanced the State's regulatory framework for State and local government cybersecurity. Among other things and broadly speaking, the Acts:

- authorized funds to be transferred from DPA in fiscal 2023 to implement the Acts;
- required that, for fiscal 2024, the Governor include in the annual budget bill an appropriation of at least 20% of the aggregated amount appropriated for information technology (IT) and cybersecurity resources in the annual budget bill for fiscal 2023;
- codified the Maryland Cyber Defense Initiative (which established the Office of Security Management (OSM) within DoIT and the Maryland Cybersecurity Coordinating Council (MCCC)) and expanded the responsibilities of OSM and MCCC;
- established the positions of Director of State Cybersecurity and Director of Local Cybersecurity within OSM;
- created the Modernize Maryland Oversight Committee (MMOC) to, among other things, advise the Secretary of Information Technology on a strategic roadmap with a timeline and budget that will (1) require updates to and investments in critical IT and cybersecurity systems, as specified, to be completed by December 31, 2025, as specified, and (2) require all updates to and investments in IT and cybersecurity to be made by December 31, 2030;
- required State and local governments to conduct cybersecurity preparedness assessments within specified timeframes;
- required DoIT to develop a centralization transition strategy toward cybersecurity centralization;
- required development of a statewide cybersecurity master plan as well as the Governor to include an appropriation in the annual budget bill in an amount necessary to cover the costs of implementing the plan without the need for DoIT to operate a charge-back model for cybersecurity services provided to State and local agencies;
- codified the Cybersecurity Preparedness Unit within the Maryland Department of Emergency Management (MDEM) and included budgetary staffing specifications for the unit;
- created a Local Cybersecurity Support Fund to assist local governments with cybersecurity costs; and
- required DoIT to hire a contractor to conduct a performance and capacity assessment to evaluate the department's capacity to implement the Acts.

The bill makes various changes to this regulatory framework. Specifically, the bill:

- requires that for fiscal 2025, and each fiscal year thereafter, the Governor must include in the annual budget bill an appropriation that is at least 20% of the aggregated amount appropriated for IT resources in the annual budget bill for the prior fiscal year for DPA for cybersecurity;
- requires that appropriations to DPA supplement, and not supplant, any existing funds in DPA for cybersecurity that may have accrued from a prior fiscal year;
- requires that, if an agency does not remediate its cybersecurity assessment findings to become compliant with State minimum cybersecurity standards by July 1, 2024, DoIT onboard the agency to its cybersecurity services and ensure OSM staff have administrative privileges to the agency's IT assets;
- specifies that the head of the Cyber Preparedness Unit within MDEM is the Director of Cybersecurity Preparedness and expressly requires the director to work in coordination with the Director of Local Cybersecurity in OSM to provide technical assistance, coordinate resources, and improve cybersecurity preparedness for units of local government;
- repeals the requirement that the SCISO be supervised by the Secretary of Information Technology and serve as the chief information security officer of DoIT, and instead simply requires the SCISO to be supervised by the Governor;
- repeals the qualification that the SCISO must, at minimum, hold a bachelor's degree;
- transfers specified cybersecurity-related duties from the Secretary of Information Technology to the SCISO, Director of State Cybersecurity, and Director of Local Cybersecurity;
- repeals specific budgetary mandates for the Cyber Preparedness Unit in MDEM and instead requires the Governor to include in the annual budget bill an appropriation sufficient for five positions in the unit;
- repeals the requirement that local governments report cybersecurity incidents to the Maryland Joint Operations Center in MDEM and specifies that any such information reported by a local government may not be used by the State as a basis for imposing a fine, restricting funding, or otherwise penalizing the local government;
- requires the security policy, standards, and guidance documents developed by OSM to be consistent with a widely recognized security standard, including specified examples, instead of being consistent with best practices developed by the National Institute of Standards and Technology;
- expands the membership of MMOC and requires MMOC to advise the SCISO in addition to the Secretary of Information Technology;

- requires the IT investment framework developed by DoIT to include foundational IT projects that impact multiple units of State government;
- requires the contractors hired by DoIT to assess its performance and capacity to implement Chapters 241, 242, and 243 to provide quarterly updates on its work to the cochairs of the Joint Committee on Cybersecurity, Information Technology, and Biotechnology;
- requires the report submitted by MMOC in calendar 2024 to include an evaluation of the services provided by DoIT and an assessment of whether those services meet the needs of the agencies being served;
- requires MMOC to report, by November 1, 2023, to the General Assembly on recommendations to improve the format for the Secretary of Information Technology to report on major IT development projects to meet the needs for strategic planning and investment; and
- requires DoIT to hire an independent contractor to review the efficiency and effectiveness of foundational IT projects that impact multiple units of State government and, by November 1, 2023, report its findings and recommendations to the General Assembly.

### **State Fiscal Effect:**

#### *Dedicated Purpose Account Funding*

Chapters 241, 242, and 243 require the Governor to include in the annual budget bill for fiscal 2024 an appropriation of at least 20% of the aggregated amount appropriated for IT and cybersecurity resources in the annual budget bill for fiscal 2023. The fiscal 2024 budget as introduced includes \$152.0 million for DPA to meet the mandated appropriations required for Chapters 241, 242, and 243. DoIT processed a fiscal 2023 budget amendment to transfer \$94.0 million from DPA for remediation of State and local governments' cybersecurity. Although DoIT typically provides services on a reimbursable basis, these funds will enable DoIT to provide the remediation services at no cost to State and local government agencies, consistent with the requirements of Chapters 241, 242, and 243 and of this bill.

The bill includes a similar mandatory annual appropriation beginning in fiscal 2025. Specifically, for fiscal 2025, and each fiscal year thereafter, the Governor must include in the annual budget bill an appropriation in an amount that is not less than 20% of the aggregated amount appropriated for IT resources in the annual budget bill for the prior fiscal year for DPA for cybersecurity.

A preliminary analysis conducted by the Department of Budget and Management and the Department of Legislative Services (DLS) estimates that the aggregated amount

appropriated for IT resources in the annual budget bill for fiscal 2024 is \$868.1 million. Therefore, assuming similar amounts in future fiscal years and including the additional DPA funding in the calculations, the mandated appropriation provision requires the following amount of general funds to be appropriated for cybersecurity in DPA for the following years: \$173.6 million for fiscal 2025; \$208.4 million for fiscal 2026; \$250.0 million for fiscal 2027; and \$300.0 million for fiscal 2028. The mandated appropriation accelerates each succeeding year due to the compounding effect such that it reaches \$1.1 billion in fiscal 2035.

### *Department of Information Technology*

The bill affects DoIT's operations and finances in two major ways. First, DoIT experiences direct costs for the additional reports and responsibilities required by the bill. Second, DoIT may experience costs associated with operational restructuring as the SCISO begins to be supervised directly by the Governor instead of by the Secretary of Information Technology.

*Responsibilities and Reports:* The fiscal and policy notes for Chapters 241, 242, and 243 estimated that, to handle the substantial additional responsibilities required by that legislation, DoIT required more than 40 additional staff. The provisions of this bill generally clarify and/or modestly expand responsibilities first assigned by Chapters 241, 242, and 243. The fiscal 2024 budget, as introduced, includes authorization and funding for more than 20 new positions, presumably as the first phase in providing DoIT with the staff it needs to address new responsibilities. Given the relatively modest changes made by the bill, DLS advises that the new staff positions can likely handle the additional responsibilities for DoIT and the SCISO required by the bill, including the additional report that must be completed by MMOC. To the extent that even more staff are necessary, DoIT expenditures increase accordingly. DPA monies may be able to be used for any such additional staffing.

The bill also requires DoIT to hire an independent contractor to evaluate State projects that affect multiple units of State government. DoIT anticipates these evaluations to include substantial technical work. Moreover, due to the extremely tight timeframe in which the evaluation must be completed (the report is due November 1, 2023), DoIT anticipates the total cost for the evaluations to be \$5.0 million. For purposes of this analysis, due to the bill's June 1, 2023 effective date, it is assumed that general fund expenditures for DoIT increase by \$1.0 million in fiscal 2023 and \$4.0 million in fiscal 2024. DLS notes that it is unlikely that DPA funding can be used for these evaluations as they are not directly related to cybersecurity.

*State Chief Information Security Officer Supervision:* DoIT and the SCISO may experience administrative costs related to the transfer of the SCISO and OSM from under the supervision of the Secretary of Information Technology to the Governor. For purposes

of this analysis, it is assumed that DoIT and OSM can continue to co-locate under their current arrangement and that no additional office space or administrative staff are needed, especially because there is substantial overlap between the responsibilities of DoIT and OSM. There may be costs associated with the development of agreements and memoranda of understanding to ensure the co-location and sharing of administrative staff can take place. To the extent that additional space or administrative staff are needed, general fund expenditures increase accordingly.

*Maryland Department of Emergency Management*

The fiscal 2024 budget as introduced includes more staff and funding for the Cyber Preparedness Unit than the five-staff minimum established by Chapters 241, 242, and 243; specifically, it includes funding for five full-time positions and two contractual positions. Therefore, the repeal of the minimum staffing and funding requirement is not anticipated to affect MDEM’s operations or finances. However, MDEM does not currently have a director for the unit, as the unit reports to other directors within MDEM’s organizational structure. MDEM advises that it plans to categorize the position established by the bill as a branch manager, rather than a director.

Therefore, general fund expenditures for MDEM increase by \$158,307 in fiscal 2024, which assumes no effect in fiscal 2023 despite the bill’s June 1, 2023 effective date and that the branch manager is hired on October 1, 2023. This estimate reflects the cost of hiring one full-time permanent branch manager to lead the Cyber Preparedness Unit. It includes a salary, fringe benefits, one-time start-up costs, and ongoing operating expenses. It also includes travel reimbursement costs for unit staff and a one-time cost for various cybersecurity training courses.

Position	1.0
Salary and Fringe Benefits	\$95,890
Cyber Training Courses	50,000
Other Operating Expenses	<u>12,417</u>
<b>Total FY 2024 MDEM Expenditures</b>	<b>\$158,307</b>

Future year expenditures reflect a full salary with annual increases and employee turnover as well as annual increases in ongoing operating expenses and termination of one-time costs.

This analysis assumes general fund expenditures continue to be used for MDEM’s Cyber Preparedness Unit. However, DPA monies may be able to be used for this purpose instead.

## *State Agency Cybersecurity Service Onboarding*

The bill requires that, if an agency does not remediate its cybersecurity assessment findings to become compliant with State minimum cybersecurity standards by July 1, 2024, then DoIT must onboard the agency to its cybersecurity services and ensure OSM staff have administrative privileges to the agency's IT assets. Since current law generally requires DoIT to provide cybersecurity services without the need to use a charge-back model, to the extent any State agencies must be onboarded beginning as early as fiscal 2025, monies held in DPA for cybersecurity are assumed to be used by DoIT to complete the onboarding process and manage any affected agencies' cybersecurity services. Accordingly, special fund expenditures may increase beginning in fiscal 2025. Any such impact, however, cannot be reliably predicted or quantified without actual experience under the bill.

---

### **Additional Information**

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

**Designated Cross File:** HB 1065 (Delegate Kaiser, *et al.*) - Health and Government Operations.

**Information Source(s):** Department of Information Technology; Maryland Department of Emergency Management; Governor's Office; Department of Budget and Management; Department of Public Safety and Correctional Services; Department of Legislative Services

**Fiscal Note History:** First Reader - March 13, 2023  
km/mcr

---

Analysis by: Richard L. Duncan

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