SB 825

Department of Legislative Services

Maryland General Assembly
2026 Session

FISCAL AND POLICY NOTE
First Reader

Senate Bill 825 (Senator Hester)
Education, Energy, and the Environment

Public Safety - Critical Infrastructure Protection

This bill establishes a Critical Infrastructure Protection Branch in the Maryland Coordination and Analysis Center (MCAC) to identify current and potential threats to the State's critical infrastructure and prioritize the State's critical infrastructure assets, as specified. The executive director of MCAC must appoint a Chief Critical Infrastructure Officer for the branch and the Maryland Department of Emergency Management (MDEM), in consultation with MCAC, must coordinate consequence management efforts and respond to an attack on the State's critical infrastructure. The Department of Information Technology (DoIT), in consultation with MCAC, must (1) allow the owner or operator of critical infrastructure to become a member of the Maryland Information Sharing and Analysis Center, and (2) provide up-to-date cybersecurity reporting standards to an owner or operator of critical infrastructure. **The bill takes effect July 1, 2026.**

Fiscal Summary

State Effect: General fund expenditures increase by $315,400 in FY 2027 for staffing; future years reflect annualization and ongoing operating expenses. Revenues are not affected.

(in dollars)	FY 2027	FY 2028	FY 2029	FY 2030	FY 2031
Revenues	$0	$0	$0	$0	$0
GF Expenditure	315,400	374,700	391,900	409,500	427,400
Net Effect	($315,400)	($374,700)	($391,900)	($409,500)	($427,400)

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

Local Effect: The bill is not anticipated to materially affect local government operations or finances.

Small Business Effect: None.

Analysis

Bill Summary: "Critical infrastructure" means assets, systems, and networks, whether physical or virtual, considered by the U.S. Department of Homeland Security to be so vital to the United States that their incapacitation or destruction would have a debilitating effect on one or more of the following (1) security; (2) national economic security; (3) national public health; or (4) safety.

The Chief Critical Infrastructure Officer must (1) administer and operate the branch; (2) implement the provisions of the bill; (3) direct critical infrastructure security efforts across the State; (4) coordinate with specified entities; (5) engage with critical infrastructure providers on voluntary cyber and physical assessments and provide critical infrastructure providers with best practices for security and the results of voluntary assessments; and (6) advise the Governor and the Director of the Governor's Office of Homeland Security on critical infrastructure security issues.

In carrying out its duties, the Critical Infrastructure Protection Branch must engage in specified activities, including coordinating with specified entities to determine threat levels of the State's critical infrastructure, engaging and coordinating with specified stakeholders, and strengthening the State's critical infrastructure priority assets, as specified.

Current Law:

Fusion Centers and the Maryland Coordination and Analysis Center

Fusion centers are a collaborative effort of two or more federal, State, or local government agencies that combine resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal and terrorist activity. Generally, fusion centers receive information and intelligence from a variety of sources and disseminate the information to all levels of government to identify and address immediate and emerging threats.

MCAC is the State's only fusion center and is housed in the Department of State Police (DSP). Among other responsibilities, MCAC collects and distributes domestic terrorism intelligence and analysis to federal, State, and local stakeholders and law enforcement agencies. Additional information regarding MCAC can be found on its website.

Governor's Office of Homeland Security

Established by regulation, the Governor's Office of Homeland Security is responsible for directing homeland security efforts across State government and coordinating with federal and local governments, the private sector, academia, and the public to find solutions that

ensure public safety while protecting individual freedoms. Among other things, the director of the office is responsible for advising the Governor on policies, strategies, and measures to enhance and improve the ability to detect, prevent, prepare for, protect against, respond to, and recover from man-made emergencies or disasters, including terrorist attacks. The director is also generally responsible for coordinating homeland security activities within the State and coordinating with federal and local governments.

Department of Information Technology – Generally

DoIT and the Secretary of Information Technology are responsible for, among other things: (1) developing, maintaining, revising, and enforcing information technology (IT) policies, procedures, and standards; (2) providing technical assistance, advice, and recommendations to the Governor and any unit of State government concerning IT matters; (3) reviewing agency project plans to make information and services available to the public over the Internet; and (4) developing and maintaining a statewide IT Master Plan, as specified. "Information technology" means all electronic information processing, including maintenance, telecommunications, hardware, software, and associated services.

Cybersecurity

Chapters 241, 242, and 243 of 2022 expanded and enhanced the State's regulatory framework for State and local government cybersecurity. Under the Acts, DoIT and MDEM are State agencies generally responsible for overseeing cybersecurity practices, policies, and infrastructure for the State and local governments. 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 were modified by Chapters 164 and 165 of 2025 to distinguish and clarify the responsibilities established by Chapters 241, 242, and 243 between DoIT and MDEM. Notably, and among other things, Chapters 164 and 165 (1) transferred the responsibility for supporting local governments in developing vulnerability assessments and cyber assessments from MDEM to the Office of Security Management within DoIT and (2) clarified that OSM is not responsible for assisting local government entities in the development of cybersecurity preparedness and response plans.

State Fiscal Effect: DSP advises that while MCAC has already created a Critical Infrastructure Protection Branch and appointed an officer to oversee the branch, the bill establishes new cybersecurity requirements that neither the branch nor officer can accomplish with existing resources, necessitating at least three computer network specialists to support the branch and officer. The Department of Legislative Services notes

that although the bill requires the branch and officer to *coordinate* with specified State entities, it also requires the branch and officer to accomplish certain cybersecurity functions independently.

Therefore, general fund expenditures increase by $315,361 in fiscal 2027, which accounts for a 90-day start-up delay from the bill's July 1, 2026 effective date. This estimate reflects the cost of hiring three computer network specialists to support the branch and officer in conducting the bill's specified cybersecurity requirements. It includes salaries, fringe benefits, one-time start-up costs, and ongoing operating expenses.

Positions	3.0
Salaries and Fringe Benefits	$287,939
Operating Expenses	27,422
Total FY 2027 State Expenditures	**$315,361**

Future year expenditures reflect full salaries with annual increases and employee turnover as well as annual increases in ongoing operating expenses.

DoIT advises that the bill creates new operational responsibilities beyond its current cybersecurity functions, requiring four full-time cybersecurity subject matter experts at a cost that increases to more than $700,000 by fiscal 2031. PSC advises that its responsibility to coordinate threat level determinations with the new branch requires one full-time information technology systems technical specialist at a cost that increases to approximately $149,000 by fiscal 2031. DLS disagrees and advises that while the bill requires coordination among DoIT, PSC, and the branch on determining threat levels, the bill ultimately requires the branch to engage in these activities as part of the branch's required duty to prioritize the State's critical infrastructure assets. Therefore, it is anticipated that the branch will take the lead role in coordination, and DoIT and PSC can coordinate with the branch with existing resources. However, if coordination with the branch results in a significant operational impact, DoIT and PSC may request additional resources through the annual budget process.

It is assumed that other State agencies can coordinate with the branch using existing budgeted resources. This analysis does not include potential impacts on State, local, and/or private entities that control "critical infrastructure," although the activities of the branch may have a fiscal or operational impact on those entities.

Additional Information

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

Designated Cross File: HB 1239 (Delegate Kaiser, *et al.*) - Government, Labor, and Elections.

Information Source(s): Department of Information Technology; Anne Arundel, Baltimore, Montgomery, and Prince George's counties; Maryland Department of Emergency Management; Maryland Municipal League; Governor's Office of Crime Prevention and Policy; Maryland Department of the Environment; Department of State Police; Maryland Department of Transportation; Public Service Commission; Department of Legislative Services

Fiscal Note History: First Reader - March 1, 2026
js/aad

Analysis by: Thomas S. Elder

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