SB 825

Department of Legislative Services

Maryland General Assembly
2026 Session

FISCAL AND POLICY NOTE
Third Reader - Revised

Senate Bill 825 (Senator Hester, *et al.*)

Education, Energy, and the Environment Government, Labor, and Elections

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) must coordinate consequence management efforts and respond to cascading impacts of 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; (2) provide up-to-date cybersecurity reporting standards to an owner or operator of critical infrastructure; and (3) direct critical infrastructure cybersecurity efforts across the units of State government. **The bill takes effect July 1, 2026.**

Fiscal Summary

State Effect: None. The bill generally codifies the existing Critical Infrastructure Protection Branch within MCAC. Additionally, MDEM and DoIT advise they can handle the bill's requirements with existing resources. Revenues are not affected.

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; and (5) 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 supporting the State's critical infrastructure priority assets, as specified.

It is the intent of the General Assembly that nothing in the bill must be interpreted to supersede, abrogate, modify, limit, or otherwise affect any cybersecurity regulation, requirement, or authority that is currently in effect and that applies to critical infrastructure entities that are under federal, State, or sector-specific regulatory frameworks.

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. 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 (OSM) within DoIT and (2) clarified that OSM is not responsible for assisting local government entities in the development of cybersecurity preparedness and response plans.

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
caw/aad Third Reader - March 31, 2026
Revised - Amendment(s) - March 31, 2026

Analysis by: Thomas S. Elder

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