SENATE BILL 825

E4 6lr2098
CF HB 1239

By: ~~Senator Hester~~ **Senators Hester, Attar, Brooks, Carozza, Kagan, and Simonaire**
Introduced and read first time: February 6, 2026
Assigned to: Education, Energy, and the Environment

Committee Report: Favorable with amendments
Senate action: Adopted
Read second time: March 4, 2026

CHAPTER _____

AN ACT concerning

Public Safety – Critical Infrastructure Protection

FOR the purpose of establishing the Critical Infrastructure Protection Branch in the Maryland Coordination and Analysis Center; requiring the Department of Emergency Management, in consultation with the Center, to take certain action in response to an attack on the State's critical infrastructure; requiring the Department of Information Technology to allow the owner or operator of critical infrastructure to become a member of the Maryland Information Sharing and Analysis Center and provide certain cybersecurity reporting standards to the owner or operator; and generally relating to critical infrastructure protection.

BY adding to
Article – Public Safety
Section 14–1401 through 14–1404 to be under the new subtitle "Subtitle 14. Critical Infrastructure"
Annotated Code of Maryland
(2022 Replacement Volume and 2025 Supplement)

Preamble

~~WHEREAS, It is the government's responsibility to plan and provide for public safety, protection of public and private institutions and infrastructure, and continuity of governance; and~~

EXPLANATION: **CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.**
[Brackets**]** indicate matter deleted from existing law.
Underlining indicates amendments to bill.
~~Strike out~~ indicates matter stricken from the bill by amendment or deleted from the law by amendment.

WHEREAS, Critical infrastructure forms the backbone of Maryland's economy, public safety, and quality of life and any disruption to these systems poses a direct threat to the health, safety, and welfare of Maryland residents and visitors; and

WHEREAS, Effective protection of critical infrastructure requires coordinated planning, information sharing, and preparedness among State and local governments, private sector owners and operators, federal partners, and regional stakeholders to identify vulnerabilities, mitigate risks, and respond rapidly to emerging threats; and

WHEREAS, Maryland's proximity to the nation's capital, its many points of entry into the United States, and the multitude of high–profile targets in the Washington–Baltimore region require homeland security to be a top priority of the Governor; now, therefore,

SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND, That the Laws of Maryland read as follows:

Article – Public Safety

SUBTITLE 14. CRITICAL INFRASTRUCTURE.

14–1401.

(A) IN THIS SUBTITLE THE FOLLOWING WORDS HAVE THE MEANINGS INDICATED.

(B) "BRANCH" MEANS THE CRITICAL INFRASTRUCTURE PROTECTION BRANCH.

(C) "CENTER" MEANS THE MARYLAND COORDINATION AND ANALYSIS CENTER.

(D) (1) "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:

(I) SECURITY;

(II) NATIONAL ECONOMIC SECURITY;

(III) NATIONAL PUBLIC HEALTH; OR

(IV) SAFETY.

(2) "CRITICAL INFRASTRUCTURE" INCLUDES A HOSPITAL OR HEALTH CARE FACILITY.

(E) "EXECUTIVE DIRECTOR" MEANS THE EXECUTIVE DIRECTOR OF THE MARYLAND COORDINATION AND ANALYSIS CENTER.

14–1402.

THERE IS A CRITICAL INFRASTRUCTURE PROTECTION BRANCH IN THE MARYLAND COORDINATION AND ANALYSIS CENTER.

14–1403.

(A) THE EXECUTIVE DIRECTOR SHALL APPOINT A CHIEF CRITICAL INFRASTRUCTURE OFFICER FOR THE BRANCH.

(B) THE CHIEF CRITICAL INFRASTRUCTURE OFFICER SHALL:

(1) ADMINISTER AND OPERATE THE BRANCH, IN ACCORDANCE WITH THIS SUBTITLE;

(2) IMPLEMENT THE PROVISIONS OF THIS SUBTITLE;

(3) DIRECT CRITICAL INFRASTRUCTURE SECURITY EFFORTS ACROSS THE STATE;

(4) COORDINATE WITH:

(I) THE DIRECTOR OF THE GOVERNOR'S OFFICE OF HOMELAND SECURITY;

(II) CRITICAL <u>INFRASTRUCTURE</u> INDUSTRY, LOCAL, AND FEDERAL COUNTERPART ORGANIZATIONS; ~~AND~~

(III) <u>THE DEPARTMENT OF INFORMATION TECHNOLOGY;</u>

<u>(IV) THE NATIONAL GUARD; AND</u>

<u>(V)</u> OTHER KEY STAKEHOLDERS IDENTIFIED BY THE CHIEF CRITICAL INFRASTRUCTURE OFFICER; <u>AND</u>

(5) ~~(I) ENGAGE WITH CRITICAL INFRASTRUCTURE PROVIDERS ON~~

~~VOLUNTARY CYBER AND PHYSICAL ASSESSMENTS; AND~~

~~(II) 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.**

14–1404.

(A) THE BRANCH SHALL:

(1) IDENTIFY CURRENT AND POTENTIAL THREATS TO THE STATE'S CRITICAL INFRASTRUCTURE;

(2) PRIORITIZE THE STATE'S CRITICAL INFRASTRUCTURE ASSETS BY:

(I) IN COORDINATION WITH THE DEPARTMENT OF INFORMATION TECHNOLOGY, THE OFFICE OF SECURITY MANAGEMENT, AND THE PUBLIC SERVICE COMMISSION, DETERMINING THE THREAT LEVEL TO THE STATE'S CRITICAL INFRASTRUCTURE, FOCUSING ON FOREIGN ACTORS, DOMESTIC ACTORS, AND INSIDER THREATS;

(II) DETERMINING THE IMPACTS TO THE STATE'S CRITICAL INFRASTRUCTURE IN THE CASE OF A CYBERSECURITY OR PHYSICAL ATTACK;

(III) UNDERSTANDING THE EFFECT THAT THE COMPROMISE OF ONE ASPECT OF CRITICAL INFRASTRUCTURE MAY HAVE ON ANOTHER ASPECT OF CRITICAL INFRASTRUCTURE;

(IV) ENGAGING AND COORDINATING WITH CRITICAL INFRASTRUCTURE SECTOR LEADERS, MILITARY LEADERS, AND OTHER RELEVANT STAKEHOLDERS;

(V) IDENTIFYING THE STATE'S CRITICAL INFRASTRUCTURE OPERATIONAL TECHNOLOGY SYSTEMS; AND

(VI) ~~STRENGTHENING~~ SUPPORTING THE STATE'S CRITICAL INFRASTRUCTURE PRIORITY ASSETS BY:

1. CONNECTING PRIORITY ASSETS TO RESOURCES FOR

CONDUCTING INTEGRATED ASSESSMENTS OF THE STATE'S CRITICAL INFRASTRUCTURE TO DETECT AND DOCUMENT VULNERABILITIES AND OPERATIONAL DEPENDENCIES;

2. ~~SUPPORTING~~ IDENTIFYING TECHNICAL AND GRANT OPPORTUNITIES TO SUPPORT REMEDIATION OF IDENTIFIED VULNERABILITIES; AND

3. ~~ASSISTING IN THE COMPLETION OF VULNERABILITY REMEDIATION; AND~~ ESTABLISHING MECHANISMS TO SUPPORT SHARED LEARNING AND BEST PRACTICES BETWEEN DIFFERENT CRITICAL INFRASTRUCTURE ASSETS.

~~4. IMPLEMENTING OPERATIONAL TECHNOLOGY ARCHITECTURE MONITORING THROUGH THE MARYLAND INFORMATION SHARING AND ANALYSIS CENTER.~~

(B) THE DEPARTMENT OF EMERGENCY MANAGEMENT~~, IN CONSULTATION WITH THE CENTER,~~ SHALL COORDINATE CONSEQUENCE MANAGEMENT EFFORTS AND RESPOND TO CASCADING IMPACTS OF AN ATTACK ON THE STATE'S CRITICAL INFRASTRUCTURE, IN ACCORDANCE WITH THIS TITLE.

(C) THE DEPARTMENT OF INFORMATION TECHNOLOGY, IN CONSULTATION WITH THE CENTER, SHALL:

(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; AND

(3) DIRECT CRITICAL INFRASTRUCTURE CYBERSECURITY EFFORTS ACROSS THE UNITS OF STATE GOVERNMENT.

SECTION 2. AND BE IT FURTHER ENACTED, That it is the intent of the General Assembly that nothing in this Act shall 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.~~.~~

SECTION ~~2.~~ 3. AND BE IT FURTHER ENACTED, That this Act shall take effect July 1, 2026.