MML- FAV-HB 593.pdf
Uploaded by: Iris Ibegbulem
Position: FAV

TESTIMONY

COMMITTEE:	House Judiciary	**DATE:**	February 10, 2026
POSITION:	Favorable	**BILL:**	HB 593

The Maryland Municipal League (MML) supports House Bill 593.

HB 593 expands the definition of critical infrastructure to include systems and assets, both physical or virtual, that are vital to a municipality's operations. The incapacity or destruction of such important systems would have a harmful effect on both the public and economic security of that municipality. The bill also creates stronger penalties by making it a felony to intentionally impair or destroy critical infrastructure or a public safety answering point. When convicted, violators will face substantial penalties including imprisonment and a significant fine. This ensures that those who threaten municipal essential systems are held accountable.

The State of Maryland has been hit by bad actors before with a memorable ransomware attack on the Maryland Department of Transportation in 2025. Anna Arundel County had a cyber incident in 2025 which affected their government operations and network while Baltimore City's ransomware attack in 2019 affected the city's most critical systems. Municipalities face an elevated risk of disruption to critical systems due to limited staffing capacity to prevent, detect, and respond to cyberattacks. Being able to charge and prosecute individuals who intentionally seek to harm municipalities and the communities they serve allows municipalities to better protect critical services and systems while maintaining public trust.

For these reasons, the League respectfully requests that the committee provide House Bill 593 a favorable report.

For more information relating to this piece of testimony, please contact:

Iris Ibegbulem: Manager, Advocacy and Public Policy, irisi@mdmunicipal.org

HB0593-JUD_MACo_SUP.pdf
Uploaded by: Kevin Kinnally
Position: FAV

House Bill 593

Criminal Law - Interference With Critical Infrastructure or a Public Safety Answering Point

MACo Position: **SUPPORT**

To: Judiciary Committee

Date: February 10, 2026

From: Kevin Kinnally

The Maryland Association of Counties (MACo) **SUPPORTS** HB 593.

HB 593 bolsters Maryland's ability to prevent, deter, and respond to threats against critical infrastructure. Counties support this bill because disruptions to these systems create immediate public safety risks and can cascade across emergency response, public health, and basic services.

Counties operate and maintain essential infrastructure that underpins public safety, mobility, and basic services, including water and wastewater systems, public buildings, emergency operations facilities, transit operations, local road systems, and public safety networks. Counties also partner directly with private utilities and regional providers to coordinate security planning and emergency response.

Emergency managers plan for storms, floods, and major emergencies. But targeted disruption creates a different kind of threat, one designed to interrupt basic services and strain response capacity. This bill addresses that gap by expanding Maryland's protections for critical infrastructure and strengthening the State's ability to deter and prosecute intentional interference with essential systems.

Counties have invested heavily in resilience and continuity planning for these systems, including physical security upgrades, redundancy, and incident response coordination. HB 593 complements that work by providing clearer legal tools to address intentional interference and by reinforcing that critical infrastructure protection remains a shared priority across all levels of government.

This bill provides clear consequences for intentional interference, supports coordinated response, and protects essential systems that Maryland residents depend on. For these reasons, MACo urges the Committee to issue a **FAVORABLE** report on HB 593.

MCPA_MSA HB 593 - Interference With Critical Infra

Uploaded by: Samira Jackson

Position: FAV

Maryland Chiefs of Police Association
Maryland Sheriffs' Association

MEMORANDUM

TO: The Honorable Sandy Bartlett, Chair and
Members of the Judiciary Committee

FROM: Darren Popkin, Executive Director, MCPA-MSA Joint Legislative Committee
Andrea Mansfield, Representative, MCPA-MSA Joint Legislative Committee
Samira Jackson, Representative, MCPA-MSA Joint Legislative Committee

DATE: February 10, 2026

RE: **HB 593 - Criminal Law - Interference With Critical Infrastructure or a Public Safety Answering Point**

POSITION: **SUPPORT**

The Maryland Chiefs of Police Association (MCPA) and the Maryland Sheriffs' Association (MSA) **SUPPORT HB 593.** This bill clarifies and strengthens existing law by explicitly criminalizing intentional interference with critical infrastructure. As reflected in the bill's structure, outdated or insufficient statutory language is removed, while new provisions are added to clearly define prohibited conduct and establish appropriate criminal penalties for actions that threaten essential systems relied upon by the public every day.

Critical infrastructure, including utilities, transportation systems, communications networks, and other essential facilities, is foundational to public safety, economic stability, and emergency response. HB 593 appropriately recognizes that intentional disruption of these systems poses serious risks not only to property, but to human life. By adding clear statutory language that criminalizes interference with critical infrastructure, the bill closes gaps in current law and ensures that dangerous conduct can be addressed before it escalates into widespread harm.

MCPA and MSA support the inclusion of the bill's language into existing law and believe that intentional interference with critical infrastructure should be treated as a serious criminal offense. HB 593 strikes the appropriate balance between modernizing the statute and strengthening public safety protections. For these reasons, MCPA and MSA **SUPPORTS HB 593** and urge a **FAVORABLE** committee report.

532 Baltimore Boulevard, Suite 308
Westminster, Maryland 21157
667-314-3216 / 667-314-3236

LR 759 - Interference with Critical Infrastructure

Uploaded by: Terri Hill

Position: FAV

DRAFTER COPY

E1 6lr0759
HB 445/25 – JUD

Drafted by: Carpenter

Bill No.: _____

Requested: _____

Committee: _____

By: **Delegate Hill**

A BILL ENTITLED

AN ACT concerning

Criminal Law – Interference With Critical Infrastructure or a Public Safety Answering Point – Penalties

FOR the purpose of prohibiting a person from taking certain actions with the intent to deny access to an authorized user or interrupt or impair the functioning of critical infrastructure; prohibiting a person from taking certain actions that deny access to an authorized user or interrupt or impair the functioning of critical infrastructure or a public safety answering point; and generally relating to critical infrastructure and public safety answering points.

BY repealing and reenacting, with amendments,
Article – Criminal Law
Section 7–302(a), (c), and (d)
Annotated Code of Maryland
(2021 Replacement Volume and 2025 Supplement)

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

Article – Criminal Law

7–302.

(a) (1) In this section the following words have the meanings indicated.

EXPLANATION: **CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.**
[Brackets**]** indicate matter deleted from existing law.

(2) "Access" means to instruct, communicate with, store data in, retrieve or intercept data from, or otherwise use the resources of a computer program, computer system, or computer network.

(3) (i) "Aggregate amount" means a direct loss of property or services incurred by a victim.

(ii) "Aggregate amount" includes:

1. the value of any money, property, or service lost, stolen, or rendered unrecoverable by the crime; or

2. any actual reasonable expenditure incurred by the victim to verify whether a computer program, computer, computer system, or computer network was altered, acquired, damaged, deleted, disrupted, or destroyed by access in violation of this section.

(4) (i) "Computer" means an electronic, magnetic, optical, organic, or other data processing device or system that performs logical, arithmetic, memory, or storage functions.

(ii) "Computer" includes property, a data storage facility, or a communications facility that is directly related to or operated with a computer.

(iii) "Computer" does not include an automated typewriter, a typesetter, or a portable calculator.

(5) "Computer control language" means ordered statements that direct a computer to perform specific functions.

(6) "Computer database" means a representation of information, knowledge, facts, concepts, or instructions that:

(i) is intended for use in a computer, computer system, or computer network; and

(ii) 1. is being prepared or has been prepared in a formalized manner; or

2. is being produced or has been produced by a computer, computer system, or computer network.

(7) "Computer network" means the interconnection of one or more computers through:

(i) the use of a satellite, microwave, line, or other communication medium; and

(ii) terminals or a complex consisting of two or more interconnected computers regardless of whether the interconnection is continuously maintained.

(8) "Computer program" means an ordered set of instructions or statements that may interact with related data and, when executed in a computer system, causes a computer to perform specified functions.

(9) "Computer services" includes computer time, data processing, and storage functions.

(10) "Computer software" means a computer program, instruction, procedure, or associated document regarding the operation of a computer system.

(11) "Computer system" means one or more connected or unconnected computers, peripheral devices, computer software, data, or computer programs.

(12) **"CRITICAL INFRASTRUCTURE" MEANS SYSTEMS AND ASSETS, WHETHER PHYSICAL OR VIRTUAL, THAT ARE SO VITAL TO THE STATE, A COUNTY, OR A MUNICIPALITY THAT THE INCAPACITY OR DESTRUCTION OF ONE OR MORE COMPONENTS WOULD HAVE A DEBILITATING IMPACT ON:**

(I) PUBLIC SECURITY;

(II) ECONOMIC SECURITY;

(III) PUBLIC HEALTH;

(IV) PUBLIC SAFETY;

(V) PUBLIC TRANSPORTATION; OR

(VI) PUBLIC UTILITIES.

(13) "Ransomware" means a computer or data contaminant, encryption, or lock that:

(i) is placed or introduced without authorization into a computer, a computer network, or a computer system; and

(ii) restricts access by an authorized person to a computer, computer data, a computer network, or a computer system in a manner that results in the person responsible for the placement or introduction of the contaminant, encryption, or lock demanding payment of money or other consideration to remove the contaminant, encryption, or lock.

(c) (1) A person may not intentionally, willfully, and without authorization:

(i) access, attempt to access, cause to be accessed, or exceed the person's authorized access to all or part of a computer network, computer control language, computer, computer software, computer system, computer service, or computer database; or

(ii) copy, attempt to copy, possess, or attempt to possess the contents of all or part of a computer database accessed in violation of item (i) of this paragraph.

(2) A person may not commit an act prohibited by paragraph (1) of this subsection with the intent to:

(i) cause the malfunction or interrupt the operation of all or any part of a computer, computer network, computer control language, computer software, computer system, computer service, or computer data; or

(ii) alter, damage, or destroy all or any part of data or a computer program stored, maintained, or produced by a computer, computer network, computer software, computer system, computer service, or computer database.

(3) A person may not intentionally, willfully, and without authorization:

(i) possess, identify, or attempt to identify a valid access code; or

(ii) publicize or distribute a valid access code to an unauthorized person.

(4) A person may not commit an act prohibited under this subsection with the intent to interrupt or impair the functioning of:

(i) the State government;

(ii) a service, device, or system related to the production, transmission, delivery, or storage of electricity or natural gas in the State that is owned, operated, or controlled by a person other than a public service company, as defined in § 1–101 of the Public Utilities Article;

(iii) a service provided in the State by a public service company, as defined in § 1–101 of the Public Utilities Article;

(iv) a health care facility, as defined in § 18–338.1 of the Health – General Article; or

(v) a public school, as defined in § 1–101 of the Education Article.

(5) (i) This paragraph does not apply to a person who has a bona fide scientific, educational, governmental, testing, news, or other similar justification for possessing ransomware.

(ii) A person may not knowingly possess ransomware with the intent to use the ransomware for the purpose of introduction into the computer, computer network, or computer system of another person without the authorization of the other person.

(6) A person may not commit an act prohibited under this subsection with the intent to interrupt or impair the functioning of **CRITICAL INFRASTRUCTURE OR** a public safety answering point, as defined in § 1–301 of the Public Safety Article.

(7) A PERSON MAY NOT COMMIT AN ACT PROHIBITED UNDER THIS SUBSECTION THAT DENIES ACCESS TO AN AUTHORIZED USER OR INTERRUPTS OR IMPAIRS THE FUNCTIONING OF CRITICAL INFRASTRUCTURE OR A PUBLIC SAFETY ANSWERING POINT, AS DEFINED IN § 1–301 OF THE PUBLIC SAFETY ARTICLE.

(d) (1) A person who violates subsection (c)(1) of this section is guilty of a misdemeanor and on conviction is subject to imprisonment not exceeding 3 years or a fine not exceeding $1,000 or both.

(2) A person who violates subsection (c)(2) or (3) of this section:

(i) if the aggregate amount of the loss is $10,000 or more, is guilty of a felony and on conviction is subject to imprisonment not exceeding 10 years or a fine not exceeding $10,000 or both; or

(ii) if the aggregate amount of the loss is less than $10,000, is guilty of a misdemeanor and on conviction is subject to imprisonment not exceeding 5 years or a fine not exceeding $5,000 or both.

(3) A person who violates subsection (c)(4) of this section:

(i) if the aggregate amount of the loss is $10,000 or more, is guilty of a felony and on conviction is subject to imprisonment not exceeding 10 years or a fine not exceeding $100,000 or both; or

(ii) if the aggregate amount of the loss is less than $10,000, is guilty of a misdemeanor and on conviction is subject to imprisonment not exceeding 5 years or a fine not exceeding $25,000 or both.

(4) A person who violates subsection (c)(5) of this section is guilty of a misdemeanor and on conviction is subject to imprisonment not exceeding 2 years or a fine not exceeding $5,000 or both.

(5) A person who violates subsection (c)(6) of this section is guilty of a felony and on conviction is subject to imprisonment not exceeding 5 years or a fine not exceeding $25,000 or both.

(6) A PERSON WHO VIOLATES SUBSECTION (C)(7) OF THIS SECTION IS GUILTY OF A FELONY AND ON CONVICTION IS SUBJECT TO IMPRISONMENT NOT EXCEEDING 10 YEARS OR A FINE NOT EXCEEDING $50,000 OR BOTH.

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

FirstEnergy FAV - ENT - HB593 - Critical Infrastru
Uploaded by: Timothy Troxell
Position: FAV

PotomacEdison
A FirstEnergy Company

Timothy R. Troxell, CEcD
Senior Advisor, Government Affairs
301-830-0121
ttroxell@firstenergycorp.com

10802 Bower Avenue
Williamsport, MD 21795

SUPPORT – House Bill 0593
Criminal Law – Interference with Critical Infrastructure or a Public Safety Answering Point
Judiciary Committee
Tuesday, February 10, 2026

Potomac Edison, a subsidiary of FirstEnergy Corp., serves approximately 293,000 customers in all or parts of seven Maryland counties (Allegany, Carroll, Frederick, Garrett, Howard, Montgomery, and Washington). FirstEnergy is dedicated to safety, reliability, and operational excellence. Its electric distribution companies form one of the nation's largest investor-owned electric systems, serving customers in Maryland, Ohio, Pennsylvania, New Jersey, New York, and West Virginia.

Favorable

Potomac Edison / FirstEnergy supports House Bill 0593 - *Criminal Law – Interference with Critical Infrastructure or a Public Safety Answering Point*. This legislation addresses threats to actions intended to obstruct the access to, or operation of, critical infrastructure by codifying both its definition as well as the penalty for violations.

Potomac Edison / FirstEnergy requests a Favorable report on HB-593. Enhancing the security and reliability of Maryland's critical infrastructure, particularly the electric grid that serves our communities, is crucial.

The electric grid is a vital component of Maryland's critical infrastructure. It ensures the continuous delivery of electricity to homes, businesses, government agencies, and other essential services. Any intentional interference with the network could lead to significant disruptions – which can then affect public safety, economic stability, and the well-being of our customers.

House Bill 0593 aims to strengthen the legal protections against actions that intentionally disrupt or impair critical infrastructure operations. By prohibiting such actions and establishing penalties for violations, the bill serves as a deterrent against malicious activities targeting essential services. The proposed legislation also aligns with industry efforts to safeguard critical infrastructure. It complements existing measures by providing a legal framework to address intentional disruptions, thereby supporting our ability to maintain reliable electric service.

Potomac Edison / FirstEnergy believes House Bill 0593 takes a necessary step toward ensuring the security and resilience of Maryland's critical infrastructure. Given the sensitive nature of utility critical infrastructure, the need to deter actions that may harm it, and the benefits of having clearly defined penalties for taking such actions, we urge the committee to support this bill. We appreciate your consideration of our perspective on this issue and believe that protecting the essential services upon which our communities depend is vital.

For the above reasons, Potomac Edison / FirstEnergy respectfully request a Favorable vote on HB-593.