

HOUSE BILL 444

E1

5lr1162
CF 5lr1161

By: **Delegate Hill**

Introduced and read first time: January 16, 2025

Assigned to: Judiciary

A BILL ENTITLED

1 AN ACT concerning

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

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

10 BY repealing and reenacting, with amendments,
11 Article – Criminal Law
12 Section 7–302(a), (c), and (d)
13 Annotated Code of Maryland
14 (2021 Replacement Volume and 2024 Supplement)

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

17 **Article – Criminal Law**

18 7–302.

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

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

23 (3) (i) “Aggregate amount” means a direct loss of property or services
24 incurred by a victim.

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.

[Brackets] indicate matter deleted from existing law.



1 (ii) "Aggregate amount" includes:

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

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

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

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

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

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

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

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

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

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

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

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

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

31 (8) "Computer program" means an ordered set of instructions or
32 statements that may interact with related data and, when executed in a computer system,

1 causes a computer to perform specified functions.

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

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

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

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

12 (I) **PUBLIC SECURITY;**

13 (II) **ECONOMIC SECURITY;**

14 (III) **PUBLIC HEALTH; OR**

15 (IV) **PUBLIC SAFETY.**

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

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

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

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

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

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

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

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

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

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

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

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

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

15 (i) the State government;

16 (ii) a service, device, or system related to the production,
17 transmission, delivery, or storage of electricity or natural gas in the State that is owned,
18 operated, or controlled by a person other than a public service company, as defined in §
19 1–101 of the Public Utilities Article;

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

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

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

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

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

32 **(6) A PERSON MAY NOT COMMIT AN ACT PROHIBITED UNDER THIS**
33 **SUBSECTION WITH THE INTENT TO DENY ACCESS TO AN AUTHORIZED USER OR**

1 INTERRUPT OR IMPAIR THE FUNCTIONING OF CRITICAL INFRASTRUCTURE OR A
2 PUBLIC SAFETY ANSWERING POINT, AS DEFINED IN § 1-301 OF THE PUBLIC SAFETY
3 ARTICLE.

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

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

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

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

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

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

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

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

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

28 (5) A PERSON WHO VIOLATES SUBSECTION (C)(6) OF THIS SECTION IS
29 GUILTY OF A FELONY AND ON CONVICTION IS SUBJECT TO IMPRISONMENT NOT
30 EXCEEDING 5 YEARS OR A FINE NOT EXCEEDING \$25,000 OR BOTH.

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

1 SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect
2 October 1, 2025.