

# SENATE BILL 810

S2, E4, C5

2lr2965

---

By: **Senator Hester**

Introduced and read first time: February 7, 2022

Assigned to: Finance

---

## A BILL ENTITLED

1 AN ACT concerning

2 **Cybersecurity – Critical Infrastructure and Public Service Companies**  
3 **(Critical Infrastructure Security Act of 2022)**

4 FOR the purpose of authorizing the Department of Emergency Management to take action  
5 to reduce the disaster risk and vulnerability of critical infrastructure; establishing  
6 the Critical Infrastructure Cybersecurity Grant Program in the Department to  
7 leverage certain funds to make cybersecurity improvements to critical  
8 infrastructure; altering the duties and staffing requirements of the Public Service  
9 Commission to include cybersecurity; authorizing the Office of People’s Counsel to  
10 retain or hire an expert in cybersecurity; requiring certain public service companies  
11 to adopt certain cybersecurity best practices, protect certain information, include  
12 certain language in certain contracts, and establish certain security standards for  
13 certain technology devices, data, and personally identifiable information; requiring  
14 certain regulations on service quality and reliability standards for electric companies  
15 and gas companies to include cyber resiliency; and generally relating to cybersecurity  
16 risk protection of critical infrastructure and public service companies.

17 BY repealing and reenacting, with amendments,  
18 Article – Public Safety  
19 Section 14–101, 14–102(a), and 14–103  
20 Annotated Code of Maryland  
21 (2018 Replacement Volume and 2021 Supplement)

22 BY adding to  
23 Article – Public Safety  
24 Section 14–118  
25 Annotated Code of Maryland  
26 (2018 Replacement Volume and 2021 Supplement)

27 BY repealing and reenacting, without amendments,  
28 Article – Public Utilities

---

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.

[Brackets] indicate matter deleted from existing law.



1 Section 1–101(a) and 7–213(d)  
2 Annotated Code of Maryland  
3 (2020 Replacement Volume and 2021 Supplement)

4 BY adding to  
5 Article – Public Utilities  
6 Section 1–101(h–1) through (h–3) and 5–305  
7 Annotated Code of Maryland  
8 (2020 Replacement Volume and 2021 Supplement)

9 BY repealing and reenacting, with amendments,  
10 Article – Public Utilities  
11 Section 2–108(d), 2–113(a), 2–203(f), and 7–213(e)(1)  
12 Annotated Code of Maryland  
13 (2020 Replacement Volume and 2021 Supplement)

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

16 **Article – Public Safety**

17 14–101.

18 (a) In this title the following words have the meanings indicated.

19 (b) **“CRITICAL INFRASTRUCTURE” MEANS SYSTEMS AND ASSETS, WHETHER**  
20 **PHYSICAL OR VIRTUAL, THAT ARE SO VITAL TO THE STATE THAT THE INCAPACITY**  
21 **OR DESTRUCTION OF THE SYSTEM OR ASSET WOULD HAVE A DEBILITATING IMPACT**  
22 **ON ANY ONE OR COMBINATION OF THE FOLLOWING:**

23 (1) **SECURITY;**

24 (2) **ECONOMIC SECURITY;**

25 (3) **PUBLIC HEALTH; OR**

26 (4) **PUBLIC SAFETY.**

27 (c) (1) **“CYBERSECURITY” MEANS PROCESSES OR CAPABILITIES IN**  
28 **WHICH SYSTEMS, COMMUNICATIONS, AND INFORMATION ARE PROTECTED AND**  
29 **DEFENDED AGAINST DAMAGE, UNAUTHORIZED USE OR MODIFICATION, AND**  
30 **EXPLOITATION.**

31 (2) **“CYBERSECURITY” INCLUDES PROTECTING THE AVAILABILITY,**  
32 **INTEGRITY, AUTHENTICATION, CONFIDENTIALITY, AND NONREPUDIATION OF**

1 **INFORMATION.**

2 [(b)] (D) “Department” means the Maryland Department of Emergency  
3 Management.

4 [(c)] (E) “Emergency” means the imminent threat or occurrence of severe or  
5 widespread loss of life, injury, or other health impacts, property damage or destruction,  
6 social or economic disruption, or environmental degradation from natural, technological, or  
7 human-made causes.

8 [(d)] (F) (1) “Emergency management” means the planning, implementing,  
9 and conducting of risk reduction and consequence management activities across the  
10 mission areas of prevention, protection, mitigation, response, and recovery to enhance  
11 preparedness, save lives, preserve public health and safety, protect public and private  
12 property, and minimize or repair injury and damage that results or may result from  
13 emergencies.

14 (2) “Emergency management” does not include the preparation for and  
15 carrying out of functions in an emergency for which military forces are primarily  
16 responsible.

17 [(e)] (G) “Local organization for emergency management” means an  
18 organization established by a political subdivision or other local authority under § 14–109  
19 of this subtitle.

20 [(f)] (H) “Political subdivision” means a county or municipal corporation of the  
21 State.

22 [(g)] (I) “Secretary” means the Secretary of Emergency Management.

23 (J) **“SECURITY BY DESIGN” MEANS THE CONSIDERATION OF**  
24 **CYBERSECURITY RISKS IN EVERY PHASE OF A PROJECT.**

25 [(h)] (K) “Senior elected official” means:

26 (1) the mayor;

27 (2) the county executive;

28 (3) for a county that does not have a county executive, the president of the  
29 board of county commissioners or county council or other chief executive officer of the  
30 county; or

31 (4) for a municipal corporation that does not have a mayor, the burgess,  
32 chairperson, or president of the municipal governing body or other chief executive officer of  
33 the municipal corporation.

1 14–102.

2 (a) To ensure that the State will be adequately prepared to deal with emergencies,  
3 to protect the public peace, health, and safety in the State, to preserve the lives and  
4 property of the people of the State, and to ensure the social and economic resilience of the  
5 State, it is necessary to:

6 (1) establish a Maryland Department of Emergency Management;

7 (2) authorize the establishment of local organizations for emergency  
8 management in the political subdivisions;

9 (3) confer on the Governor and on the senior elected officials or governing  
10 bodies of the political subdivisions the emergency powers provided in this subtitle;

11 (4) provide for the rendering of mutual aid among the political subdivisions  
12 and with other states in carrying out emergency management functions; [and]

13 (5) authorize a comprehensive emergency management system that  
14 empowers all State departments and agencies to systematically prepare for, mitigate,  
15 respond to, and recover from potential or actual emergencies through risk reduction and  
16 consequence management; **AND**

17 **(6) AUTHORIZE THE DEPARTMENT TO ESTABLISH A GRANT PROGRAM**  
18 **FOR THE PROTECTION OF CRITICAL INFRASTRUCTURE.**

19 14–103.

20 (a) There is a Maryland Department of Emergency Management established as a  
21 principal department of the Executive Branch of State government.

22 (b) The Department has primary responsibility and authority for developing  
23 emergency management policies and is responsible for coordinating disaster risk reduction,  
24 consequence management, and disaster recovery activities.

25 (c) The Department may act to:

26 (1) reduce the disaster risk and vulnerability of persons, **CRITICAL**  
27 **INFRASTRUCTURE**, and property located in the State;

28 (2) develop and coordinate emergency planning and preparedness; and

29 (3) coordinate emergency management activities and operations:

30 (i) relating to an emergency that involves two or more State

1 agencies;

2 (ii) between State agencies and political subdivisions;

3 (iii) with local governments;

4 (iv) with agencies of the federal government and other states; and

5 (v) with private and nonprofit entities.

6 14-118.

7 (A) IN THIS SECTION, "PROGRAM" MEANS THE CRITICAL INFRASTRUCTURE  
8 CYBERSECURITY GRANT PROGRAM.

9 (B) THERE IS A CRITICAL INFRASTRUCTURE CYBERSECURITY GRANT  
10 PROGRAM IN THE DEPARTMENT.

11 (C) THE PURPOSE OF THE PROGRAM IS TO LEVERAGE FUNDS AVAILABLE  
12 FROM FEDERAL, STATE, AND LOCAL GRANT PROGRAMS TO MAKE CYBERSECURITY  
13 IMPROVEMENTS TO CRITICAL INFRASTRUCTURE.

14 (D) THE DEPARTMENT SHALL:

15 (1) ADMINISTER THE PROGRAM;

16 (2) ESTABLISH APPLICATION PROCEDURES FOR THE PROGRAM; AND

17 (3) AWARD GRANTS FROM THE PROGRAM.

18 (E) (1) IN DETERMINING THE TYPES OF CYBERSECURITY IMPROVEMENTS  
19 AND RECIPIENTS ELIGIBLE FOR GRANTS UNDER THE PROGRAM, THE DEPARTMENT  
20 SHALL:

21 (I) CONSULT WITH ELECTRIC COMPANIES, GAS COMPANIES,  
22 WATER UTILITIES, STATE AGENCIES, AND POLITICAL SUBDIVISIONS TO:

23 1. IDENTIFY CURRENT AND FORESEEABLE  
24 CYBERSECURITY RISKS TO THE STATE'S ELECTRIC GRID, NATURAL GAS  
25 INFRASTRUCTURE, AND WATER AND SEWER SYSTEMS; AND

26 2. PREPARE A REPORT ON THE CYBERSECURITY RISKS  
27 IDENTIFIED UNDER ITEM 1 OF THIS ITEM;

1                   **(II) IDENTIFY FUNDING TO FUND THE GRANTS AWARDED UNDER**  
2 **THE PROGRAM; AND**

3                   **(III) DEVELOP CRITERIA FOR SELECTING GRANT RECIPIENTS**  
4 **BASED ON A GRANT APPLICANT’S CYBERSECURITY RISK.**

5                   **(2) ON OR BEFORE DECEMBER 1, 2022, THE DEPARTMENT SHALL**  
6 **SUBMIT THE REPORT PREPARED UNDER PARAGRAPH (1)(I)2 OF THIS SUBSECTION**  
7 **TO THE GOVERNOR AND, IN ACCORDANCE WITH § 2-1257 OF THE STATE**  
8 **GOVERNMENT ARTICLE, THE GENERAL ASSEMBLY.**

9           **(F) THE DEPARTMENT SHALL:**

10                   **(1) REQUIRE EACH GRANT RECIPIENT TO DEVELOP PROCESSES TO**  
11 **ADDRESS CYBERSECURITY RISKS AND SUBMIT A REPORT ON IMPLEMENTED**  
12 **PROCESSES TO THE DEPARTMENT; AND**

13                   **(2) REQUIRE GRANT RECIPIENTS THAT MODERNIZE OR IMPROVE THE**  
14 **RESILIENCE OF ELECTRIC GRIDS, NATURAL GAS INFRASTRUCTURE, OR WATER AND**  
15 **SEWER SYSTEMS TO:**

16                   **(I) SUBMIT A REPORT ON IMPLEMENTED SECURITY BY DESIGN**  
17 **PRINCIPLES TO THE DEPARTMENT; AND**

18                   **(II) ESTABLISH A CYBERSECURITY PLAN THAT ADDRESSES**  
19 **CYBERSECURITY RISKS IN POLICY, SOFTWARE DEVELOPMENT, HARDWARE, AND**  
20 **NETWORKS.**

21                                   **Article – Public Utilities**

22 1–101.

23           (a) In this division the following words have the meanings indicated.

24                   **(H-1) “CYBER RESILIENCY” MEANS THE ABILITY TO ANTICIPATE, WITHSTAND,**  
25 **RECOVER FROM, AND ADAPT TO ADVERSE CONDITIONS, STRESSES, ATTACKS, OR**  
26 **COMPROMISES ON SYSTEMS THAT USE OR ARE ENABLED BY A CYBER RESOURCE.**

27                   **(H-2) “CYBER RESOURCE” MEANS AN INFORMATION SOURCE THAT:**

28                   **(1) CREATES, STORES, PROCESSES, MANAGES, TRANSMITS, OR**  
29 **DISPOSES OF INFORMATION IN AN ELECTRONIC FORMAT; AND**

30                   **(2) CAN BE ACCESSED BY A NETWORK OR BY USING NETWORKING**

1 **METHODS.**

2 **(H-3) “CYBERSECURITY” HAS THE MEANING STATED IN § 14-101 OF THE**  
3 **PUBLIC SAFETY ARTICLE.**

4 2-108.

5 (d) (1) The State budget shall provide sufficient money for the Commission to  
6 hire, develop, and organize a staff to perform the functions of the Commission, including  
7 analyzing data submitted to the Commission and participating in proceedings as provided  
8 in § 3-104 of this article.

9 (2) (i) As the Commission considers necessary, the Commission shall  
10 hire experts including economists, cost of capital experts, rate design experts, accountants,  
11 engineers, transportation specialists, and lawyers.

12 (ii) To assist in the regulation of intrastate hazardous liquid  
13 pipelines under Title 11, Subtitle 2 of this article, the Commission shall include on its staff  
14 at least one engineer who specializes in the storage of and the transportation of hazardous  
15 liquid materials by pipeline.

16 (3) **THE COMMISSION SHALL INCLUDE ON ITS STAFF ONE OR MORE**  
17 **EMPLOYEES DEDICATED TO CYBERSECURITY POLICY, STRATEGY, AUDITING, AND**  
18 **REPORTING.**

19 (4) The Commission may retain on a case by case basis additional experts  
20 as required for a particular matter.

21 ~~[(4)]~~ (5) The lawyers who represent the Commission staff in proceedings  
22 before the Commission shall be appointed by the Commission and shall be organized and  
23 operate independently of the office of General Counsel.

24 ~~[(5)]~~ (6) (i) As required, the Commission shall hire public utility law  
25 judges.

26 (ii) Public utility law judges are a separate organizational unit and  
27 shall report directly to the Commission.

28 ~~[(6)]~~ (7) The Commission shall hire personal staff members for each  
29 commissioner as required to provide advice, draft proposed orders and rulings, and perform  
30 other personal staff functions.

31 ~~[(7)]~~ (8) Subject to § 3-104 of this article, the Commission may delegate  
32 to a commissioner or personnel the authority to perform an administrative function  
33 necessary to carry out a duty of the Commission.

1                    **[(8)] (9)**        (i)        Except as provided in subparagraph (ii) of this paragraph  
2 or otherwise by law, all personnel of the Commission are subject to the provisions of the  
3 State Personnel and Pensions Article.

4                    (ii)        The following are in the executive service, management service,  
5 or are special appointments in the State Personnel Management System:

- 6                    1.        each commissioner of the Commission;
- 7                    2.        the Executive Director;
- 8                    3.        the General Counsel and each assistant general counsel;
- 9                    4.        the Executive Secretary;
- 10                   5.        the commissioners' personal staff members;
- 11                   6.        the chief public utility law judge; and
- 12                   7.        each license hearing officer.

13 2–113.

14            (a)        (1)        The Commission shall:

15                    (i)        supervise and regulate the public service companies subject to  
16 the jurisdiction of the Commission to:

- 17                    1.        ensure their operation in the interest of the public; and
- 18                    2.        promote adequate, economical, and efficient delivery of  
19 utility services in the State without unjust discrimination; and

20                    (ii)        enforce compliance with the requirements of law by public  
21 service companies, including requirements with respect to financial condition,  
22 capitalization, franchises, plant, manner of operation, rates, and service.

23                    (2)        In supervising and regulating public service companies, the  
24 Commission shall consider:

- 25                    (i)        the public safety;
- 26                    (ii)        the economy of the State;
- 27                    (iii)        the maintenance of fair and stable labor standards for affected  
28 workers;



1 (iv) the conservation of natural resources;

2 (v) the preservation of environmental quality, including protection  
3 of the global climate from continued short-term and long-term warming based on the best  
4 available scientific information recognized by the Intergovernmental Panel on Climate  
5 Change; [and]

6 (vi) the achievement of the State's climate commitments for reducing  
7 statewide greenhouse gas emissions, including those specified in Title 2, Subtitle 12 of the  
8 Environment Article; AND

9 (V) THE CYBERSECURITY RISKS FACED BY PUBLIC SERVICE  
10 COMPANIES IN THE STATE.

11 2-203.

12 (f) The Office of People's Counsel may retain as necessary for a particular matter  
13 or hire experts in the field of:

14 (1) utility regulation, including cost of capital experts, rate design experts,  
15 accountants, economists, engineers, transportation specialists, and lawyers; [and]

16 (2) climate change, including meteorologists, oceanographers, ecologists,  
17 foresters, geologists, seismologists, botanists, and experts in any other field of science that  
18 the People's Counsel determines is necessary; AND

19 (3) CYBERSECURITY.

20 5-305.

21 (A) IN THIS SECTION, "ZERO TRUST" MEANS A CYBERSECURITY APPROACH:

22 (1) FOCUSED ON CYBERSECURITY RESOURCE PROTECTION; AND

23 (2) BASED ON THE PREMISE THAT TRUST IS NEVER GRANTED  
24 IMPLICITLY BUT MUST BE CONTINUALLY EVALUATED.

25 (B) THIS SECTION DOES NOT APPLY TO A PUBLIC SERVICE COMPANY THAT  
26 IS:

27 (1) A COMMON CARRIER; OR

28 (2) A TELEPHONE COMPANY.

29 (C) EACH PUBLIC SERVICE COMPANY SHALL:

1           **(1) ADOPT CYBERSECURITY BEST PRACTICES, INCLUDING**  
2 **IMPLEMENTING ZERO TRUST PRINCIPLES;**

3           **(2) PROTECT PERSONALLY IDENTIFIABLE INFORMATION OF**  
4 **CUSTOMERS AND EMPLOYEES;**

5           **(3) INCLUDE IN CONTRACTS WITH THIRD-PARTY INFORMATION**  
6 **TECHNOLOGY OR OPERATIONAL TECHNOLOGY PROVIDERS PROVISIONS REQUIRING**  
7 **THE THIRD-PARTY PROVIDERS TO:**

8                   **(I) COLLECT AND PRESERVE DATA FOR CYBERSECURITY**  
9 **ANALYSIS; AND**

10                   **(II) SHARE THAT DATA AND REPORT ANY CYBERSECURITY**  
11 **BREACHES TO THE PUBLIC SERVICE COMPANY;**

12           **(4) ESTABLISH MINIMUM SECURITY STANDARDS FOR INFORMATION**  
13 **TECHNOLOGY AND OPERATIONAL TECHNOLOGY DEVICES; AND**

14           **(5) ENCRYPT AND CREATE MINIMUM SECURITY STANDARDS FOR**  
15 **DATA AND PERSONALLY IDENTIFIABLE INFORMATION HELD BY THE PUBLIC**  
16 **SERVICE COMPANY.**

17 7-213.

18           (d) On or before July 1, 2012, the Commission shall adopt regulations that  
19 implement service quality and reliability standards relating to the delivery of electricity to  
20 retail customers by electric companies through their distribution systems, using:

21           (1) SAIFI;

22           (2) SAIDI; and

23           (3) any other performance measurement that the Commission determines  
24 to be reasonable.

25           (e) (1) The regulations adopted under subsection (d) of this section shall:

26                   (i) include service quality and reliability standards, including  
27 standards relating to:

28                           1. service interruption;

29                           2. downed wire response;

- 1                                   3.     customer communications;
- 2                                   4.     vegetation management;
- 3                                   5.     periodic equipment inspections;
- 4                                   6.     annual reliability reporting; [and]
- 5                                   7.     **CYBER RESILIENCY; AND**
- 6                                   8.     any other standards established by the Commission;
- 7                                   (ii)    account for major outages caused by events outside the control of
- 8     an electric company; and
- 9                                   (iii)   for an electric company that fails to meet the applicable service
- 10   quality and reliability standards, require the electric company to file a corrective action
- 11   plan that details specific actions the company will take to meet the standards.

12                   SECTION 2. AND BE IT FURTHER ENACTED, That on or before June 31, 2023,  
13   the Public Service Commission shall update the regulations adopted under § 7–213(d) of  
14   the Public Utilities Article to include service quality and reliability standards for cyber  
15   resiliency.

16                   SECTION 3. AND BE IT FURTHER ENACTED, That this Act shall take effect June  
17   1, 2022.