

HOUSE BILL 1420

S2, C5

4lr3277

By: **Delegate Kaiser**

Introduced and read first time: February 9, 2024

Assigned to: Health and Government Operations

A BILL ENTITLED

1 AN ACT concerning

2 **Cybersecurity – Office of People’s Counsel, Public Service Companies, Public**
3 **Service Commission, and Maryland Cybersecurity Council**

4 FOR the purpose of requiring the Office of People’s Counsel to hire at least a certain number
5 of assistant people’s counsel with cybersecurity expertise to perform certain duties;
6 requiring certain public service companies to engage with a third party to conduct
7 an assessment that analyzes certain critical software; requiring a certain
8 certification to be submitted to the Office of People’s Counsel; requiring certain
9 regulations adopted by the Public Service Commission to include cyber resilience;
10 defining “critical infrastructure” for certain provisions relating to the Maryland
11 Cybersecurity Council; and generally relating to cybersecurity.

12 BY repealing and reenacting, without amendments,
13 Article – Public Utilities
14 Section 2–203(a)(1) and 7–213(d)
15 Annotated Code of Maryland
16 (2020 Replacement Volume and 2023 Supplement)

17 BY repealing and reenacting, with amendments,
18 Article – Public Utilities
19 Section 2–203(a)(2), 5–306, and 7–213(a) and (e)(1)
20 Annotated Code of Maryland
21 (2020 Replacement Volume and 2023 Supplement)

22 BY repealing and reenacting, with amendments,
23 Article – State Government
24 Section 9–2901(a)
25 Annotated Code of Maryland
26 (2021 Replacement Volume and 2023 Supplement)

27 BY repealing and reenacting, without amendments,

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.

[Brackets] indicate matter deleted from existing law.



1 Article – State Government
2 Section 9–2901(b) and (j)
3 Annotated Code of Maryland
4 (2021 Replacement Volume and 2023 Supplement)

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

7 **Article – Public Utilities**

8 2–203.

9 (a) (1) The State budget shall provide sufficient money for the Office of
10 People’s Counsel to hire necessary staff in addition to the staff assistance that is provided
11 under § 2–205(c)(2) of this subtitle.

12 (2) The Office of People’s Counsel shall hire:

13 (I) at least one assistant people’s counsel who will focus on
14 environmental issues; AND

15 (II) AT LEAST ONE ASSISTANT PEOPLE’S COUNSEL WITH
16 CYBERSECURITY EXPERTISE TO:

17 1. ADVISE THE PEOPLE’S COUNSEL ON MEASURES TO
18 IMPROVE OVERSIGHT OF THE CYBERSECURITY PRACTICES OF PUBLIC SERVICE
19 COMPANIES;

20 2. CONSULT WITH THE OFFICE OF SECURITY
21 MANAGEMENT ON CYBERSECURITY ISSUES RELATED TO UTILITY REGULATION;

22 3. ASSIST THE OFFICE OF PEOPLE’S COUNSEL IN
23 MONITORING THE MINIMUM SECURITY STANDARDS DEVELOPED UNDER § 5–306 OF
24 THIS ARTICLE;

25 4. PARTICIPATE IN BRIEFINGS TO DISCUSS
26 CYBERSECURITY PRACTICES BASED ON:

27 A. APPLICABLE NATIONAL ASSOCIATION OF
28 REGULATORY UTILITY COMMISSIONERS GUIDANCE; AND

29 B. IMPROVEMENTS TO CYBERSECURITY PRACTICES
30 RECOMMENDED IN THE CYBERSECURITY ASSESSMENTS REQUIRED UNDER § 5–306
31 OF THIS ARTICLE; AND

1 **5. SUPPORT PUBLIC SERVICE COMPANIES THAT DO NOT**
2 **MEET MINIMUM SECURITY STANDARDS WITH REMEDIATING VULNERABILITIES OR**
3 **ADDRESSING CYBERSECURITY ASSESSMENT FINDINGS.**

4 5–306.

5 (a) **(1)** In this section[, “zero–trust” means a cybersecurity approach:

6 (1) focused on cybersecurity resource protection; and

7 (2) based on the premise that trust is never granted implicitly but must be
8 continually evaluated.] **THE FOLLOWING WORDS HAVE THE MEANINGS INDICATED.**

9 **(2) “CRITICAL SOFTWARE” MEANS ANY SOFTWARE THAT HAS, OR HAS**
10 **DIRECT SOFTWARE DEPENDENCIES ON, ONE OR MORE COMPONENTS WITH AT LEAST**
11 **ONE OF THE FOLLOWING ATTRIBUTES:**

12 **(I) THE ABILITY TO RUN WITH ELEVATED PRIVILEGE OR TO**
13 **MANAGE PRIVILEGES;**

14 **(II) DIRECT OR PRIVILEGED ACCESS TO NETWORKING OR**
15 **COMPUTING RESOURCES;**

16 **(III) THE ABILITY TO CONTROL ACCESS TO DATA OR**
17 **OPERATIONAL TECHNOLOGY;**

18 **(IV) THE ABILITY TO PERFORM A FUNCTION CRITICAL TO TRUST;**
19 **OR**

20 **(V) THE ABILITY TO OPERATE OUTSIDE NORMAL TRUST**
21 **BOUNDARIES WITH PRIVILEGED ACCESS.**

22 **(3) “SUPPLY CHAIN RISK” MEANS A RISK THAT AN ADVERSARY MAY**
23 **SABOTAGE, MALICIOUSLY INTRODUCE UNWANTED FUNCTION TO, EXTRACT DATA**
24 **FROM, OR OTHERWISE SUBVERT THE DESIGN, INTEGRITY, MANUFACTURING,**
25 **PRODUCTION, DISTRIBUTION, INSTALLATION, OPERATION, MAINTENANCE,**
26 **DISPOSITION, OR RETIREMENT OF A SYSTEM OR ITEM OF SUPPLY SO AS TO SURVEIL,**
27 **DENY, DISRUPT, OR OTHERWISE MANIPULATE THE FUNCTION, USE, OR OPERATION**
28 **OF THE SYSTEM OR ITEM OF SUPPLY OR INFORMATION STORED OR TRANSMITTED**
29 **BY OR THROUGH THE SYSTEM OR ITEM OF SUPPLY.**

30 **(4) “ZERO–TRUST” MEANS A CYBERSECURITY APPROACH:**

1 (I) FOCUSED ON CYBERSECURITY RESOURCE PROTECTION;
2 AND

3 (II) BASED ON THE PREMISE THAT TRUST IS NEVER GRANTED
4 IMPLICITLY BUT MUST BE CONTINUALLY EVALUATED.

5 (b) This section does not apply to a public service company that is:

6 (1) a common carrier; or

7 (2) a telephone company.

8 (c) A public service company shall:

9 (1) adopt and implement cybersecurity standards that are equal to or
10 exceed standards adopted by the Commission;

11 (2) adopt a zero-trust cybersecurity approach for on-premises services and
12 cloud-based services;

13 (3) establish minimum security standards for each operational technology
14 and information technology device based on the level of security risk for each device,
15 including [security risks associated with supply chains] **SUPPLY CHAIN RISKS**; and

16 (4) (i) on or before July 1, 2024, and on or before July 1 every other year
17 thereafter, engage a third party to conduct an assessment of operational technology and
18 information technology devices **THAT:**

19 1. IS based on:

20 [1.] **A.** the Cybersecurity and Infrastructure Security
21 Agency's Cross-Sector Cybersecurity Performance Goals; or

22 [2.] **B.** a more stringent standard that is based on the
23 National Institute of Standards and Technology security frameworks; and

24 2. **ANALYZES CRITICAL SOFTWARE USED IN THE**
25 **OPERATIONAL TECHNOLOGY AND INFORMATION TECHNOLOGY DEVICES; AND**

26 (ii) submit to the Commission **AND THE OFFICE OF PEOPLE'S**
27 **COUNSEL** certification of the public service company's compliance with standards used in
28 the assessments under item (i) of this item.

29 (d) (1) Each public service company shall report, in accordance with the
30 process established under paragraph (2) of this subsection, a cybersecurity incident,

1 including an attack on a system being used by the public service company, to the State
2 Security Operations Center in the Department of Information Technology.

3 (2) The State Chief Information Security Officer, in consultation with the
4 Commission, shall establish a process for a public service company to report cybersecurity
5 incidents under paragraph (1) of this subsection, including establishing:

6 (i) the criteria for determining the circumstances under which a
7 cybersecurity incident must be reported;

8 (ii) the manner in which a cybersecurity incident must be reported;
9 and

10 (iii) the time period within which a cybersecurity incident must be
11 reported.

12 (3) The State Security Operations Center shall immediately notify
13 appropriate State and local agencies of a cybersecurity incident reported under this
14 subsection.

15 7-213.

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

17 (2) **“CYBER RESILIENCE” MEANS THE ABILITY TO ANTICIPATE,**
18 **WITHSTAND, RECOVER FROM, AND ADAPT TO ADVERSE CONDITIONS, STRESSES,**
19 **ATTACKS, OR COMPROMISES ON SYSTEMS THAT USE OR ARE ENABLED BY CYBER**
20 **RESOURCES.**

21 ~~[(2)]~~ (3) (i) “Eligible reliability measure” means a replacement of or
22 an improvement in existing infrastructure of an electric company that:

23 1. is made on or after June 1, 2014;

24 2. is designed to improve public safety or infrastructure
25 reliability;

26 3. does not increase the revenue of an electric company by
27 connecting an improvement directly to new customers; and

28 4. is not included in the current rate base of the electric
29 company as determined in the electric company’s most recent base rate proceeding.

30 (ii) “Eligible reliability measure” includes vegetation management
31 measures that are necessary to meet applicable service quality and reliability standards
32 under this section.

1 [(3)] (4) “Fund” means the Electric Reliability Remediation Fund
2 established under subsection (j) of this section.

3 [(4)] (5) “System–average interruption duration index” or “SAIDI” means
4 the sum of the customer interruption hours divided by the total number of customers
5 served.

6 [(5)] (6) “System–average interruption frequency index” or “SAIFI”
7 means the sum of the number of customer interruptions divided by the total number of
8 customers served.

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

12 (1) SAIFI;

13 (2) SAIDI; and

14 (3) any other performance measurement that the Commission determines
15 to be reasonable.

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

17 (i) include service quality and reliability standards, including
18 standards relating to:

19 1. service interruption;

20 2. downed wire response;

21 3. customer communications;

22 4. vegetation management;

23 5. periodic equipment inspections;

24 6. annual reliability reporting; [and]

25 7. **CYBER RESILIENCE; AND**

26 [7.] 8. any other standards established by the
27 Commission;

28 (ii) account for major outages caused by events outside the control of
29 an electric company; and

1 (iii) for an electric company that fails to meet the applicable service
2 quality and reliability standards, require the electric company to file a corrective action
3 plan that details specific actions the company will take to meet the standards.

4 Article – State Government

5 9–2901.

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

7 (2) “Council” means the Maryland Cybersecurity Council.

8 **(3) “CRITICAL INFRASTRUCTURE” MEANS SYSTEMS AND ASSETS,**
9 **WHETHER PHYSICAL OR VIRTUAL, SO VITAL TO THE STATE THAT THE INCAPACITY**
10 **OR DESTRUCTION OF SUCH SYSTEMS AND ASSETS WOULD HAVE A DEBILITATING**
11 **IMPACT ON SECURITY, ECONOMIC SECURITY, PUBLIC HEALTH OR SAFETY, OR ANY**
12 **COMBINATION OF THOSE MATTERS.**

13 **[(3)] (4)** “Executive Order” means Executive Order 13636 of the President
14 of the United States.

15 (b) There is a Maryland Cybersecurity Council.

16 (j) The Council shall work with the National Institute of Standards and
17 Technology and other federal agencies, private sector businesses, and private cybersecurity
18 experts to:

19 (1) for critical infrastructure not covered by federal law or the Executive
20 Order, review and conduct risk assessments to determine which local infrastructure sectors
21 are at the greatest risk of cyber attacks and need the most enhanced cybersecurity
22 measures;

23 (2) use federal guidance to identify categories of critical infrastructure as
24 critical cyber infrastructure if cyber damage or unauthorized cyber access to the
25 infrastructure could reasonably result in catastrophic consequences, including:

26 (i) interruption in the provision of energy, water, transportation,
27 emergency services, food, or other life–sustaining services sufficient to cause a mass
28 casualty event or mass evacuations;

29 (ii) catastrophic economic damage; or

30 (iii) severe degradation of State or national security;

1 (3) assist infrastructure entities that are not covered by the Executive
2 Order in complying with federal cybersecurity guidance;

3 (4) assist private sector cybersecurity businesses in adopting, adapting,
4 and implementing the National Institute of Standards and Technology cybersecurity
5 framework of standards and practices;

6 (5) examine inconsistencies between State and federal laws regarding
7 cybersecurity;

8 (6) recommend a comprehensive State strategic plan to ensure a
9 coordinated and adaptable response to and recovery from cybersecurity attacks; and

10 (7) recommend any legislative changes considered necessary by the
11 Council to address cybersecurity issues.

12 SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect
13 October 1, 2024.