HOUSE BILL 1420

S2, C5 4lr3277

By: Delegate Kaiser

Introduced and read first time: February 9, 2024 Assigned to: Health and Government Operations

Reassigned: Economic Matters and Health and Government Operations, February 15, 2024

Committee Report: Favorable with amendments

House action: Adopted

Read second time: March 9, 2024

CHAPTER _____

IANA	://iˈcon	cerning

- Cybersecurity Office of People's Counsel, Public Service Companies, Public
 Service Commission, and Maryland Cybersecurity Council
- 4 FOR the purpose of requiring authorizing the Office of People's Counsel to retain or hire at least a certain number of assistant people's counsel with cybersecurity expertise to 5 6 perform certain duties experts in the field of cybersecurity; requiring certain public 7 service companies to engage with a third party to conduct an assessment that 8 analyzes certain critical software; requiring a certain certification to be submitted to 9 the Office of People's Counsel; requiring certain regulations adopted by the Public 10 Service Commission to include cyber resilience; defining "critical infrastructure" for 11 certain provisions relating to the Maryland Cybersecurity Council; and generally 12 relating to cybersecurity.
- 13 BY repealing and reenacting, with amendments,
- 14 Article Public Utilities
- 15 Section 2–203(f), 5–306, and 7–213(a) and (e)(1)
- 16 Annotated Code of Maryland
- 17 (2020 Replacement Volume and 2023 Supplement)
- 18 BY repealing and reenacting, without amendments,
- 19 Article Public Utilities
- Section $\frac{2-203(a)(1)}{and}$ 7–213(d)
- 21 Annotated Code of Maryland
- 22 (2020 Replacement Volume and 2023 Supplement)

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.

[Brackets] indicate matter deleted from existing law.

<u>Underlining</u> indicates amendments to bill.

Strike out indicates matter stricken from the bill by amendment or deleted from the law by amendment.

$\frac{1}{2}$	BY repealing and reenacting, with amendments, Article – Public Utilities
	111 01010 1 40010 0 01110100
$\frac{3}{4}$	Section 2–203(a)(2), 5–306, and 7–213(a) and (e)(1) Annotated Code of Maryland
$\frac{4}{5}$	(2020 Replacement Volume and 2023 Supplement)
6	BY repealing and reenacting, with amendments,
7	Article – State Government
8	Section 9–2901(a)
9	Annotated Code of Maryland
10	(2021 Replacement Volume and 2023 Supplement)
11	BY repealing and reenacting, without amendments,
12	Article – State Government
13	Section 9–2901(b) and (j)
14	Annotated Code of Maryland
15	(2021 Replacement Volume and 2023 Supplement)
16 17	SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND, That the Laws of Maryland read as follows:
18	Article - Public Utilities
19	2–203.
20 21	(f) The Office of People's Counsel may retain as necessary for a particular matter or hire experts in the field of:
22	(1) utility regulation, including cost of capital experts, rate design experts,
23	accountants, economists, engineers, transportation specialists, and lawyers; [and]
24	(2) climate change, including meteorologists, oceanographers, ecologists,
25	foresters, geologists, seismologists, botanists, and experts in any other field of science that
26	the People's Counsel determines is necessary; AND
27	(3) CYBERSECURITY.
28	(a) (1) The State budget shall provide sufficient money for the Office of
29	People's Counsel to hire necessary staff in addition to the staff assistance that is provided
30	under § 2–205(c)(2) of this subtitle.
31	(2) The Office of People's Counsel shall hire:
32	(I) at least one assistant people's counsel who will focus on
33	environmental issues; AND

1 2	(II) AT LEAST ONE ASSISTANT PEOPLE'S COUNSEL WITH CYBERSECURITY EXPERTISE TO:
3 4 5	1. ADVISE THE PEOPLE'S COUNSEL ON MEASURES TO IMPROVE OVERSIGHT OF THE CYBERSECURITY PRACTICES OF PUBLIC SERVICE COMPANIES;
6 7	2. CONSULT WITH THE OFFICE OF SECURITY MANAGEMENT ON CYBERSECURITY ISSUES RELATED TO UTILITY REGULATION;
8 9 10	3. ASSIST THE OFFICE OF PEOPLE'S COUNSEL IN MONITORING THE MINIMUM SECURITY STANDARDS DEVELOPED UNDER § 5–306 OF THIS ARTICLE;
11 12	4. PARTICIPATE IN BRIEFINGS TO DISCUSS CYBERSECURITY PRACTICES BASED ON:
13 14	A. APPLICABLE NATIONAL ASSOCIATION OF REGULATORY UTILITY COMMISSIONERS GUIDANCE; AND
15 16 17	B. IMPROVEMENTS TO CYBERSECURITY PRACTICES RECOMMENDED IN THE CYBERSECURITY ASSESSMENTS REQUIRED UNDER § 5–306 OF THIS ARTICLE; AND
18 19 20	5. SUPPORT PUBLIC SERVICE COMPANIES THAT DO NOT MEET MINIMUM SECURITY STANDARDS WITH REMEDIATING VULNERABILITIES OR ADDRESSING CYBERSECURITY ASSESSMENT FINDINGS.
21	5–306.
22	(a) (1) In this section[, "zero-trust" means a cybersecurity approach:
23	(1) focused on cybersecurity resource protection; and
24 25	(2) based on the premise that trust is never granted implicitly but must be continually evaluated.] THE FOLLOWING WORDS HAVE THE MEANINGS INDICATED.
26 27 28	(2) "CRITICAL SOFTWARE" MEANS ANY SOFTWARE THAT HAS, OR HAS DIRECT SOFTWARE DEPENDENCIES ON, ONE OR MORE COMPONENTS WITH AT LEAST ONE OF THE FOLLOWING ATTRIBUTES:
29 30	(I) THE ABILITY TO RUN WITH ELEVATED PRIVILEGE OR TO MANAGE PRIVILEGES;

29

cloud-based services:

DIRECT OR PRIVILEGED ACCESS TO NETWORKING OR 1 (II)2 **COMPUTING RESOURCES;** 3 (III) THE ABILITY TO CONTROL ACCESS TO DATA OR 4 **OPERATIONAL TECHNOLOGY;** 5 (IV) THE ABILITY TO PERFORM A FUNCTION CRITICAL TO TRUST; 6 \mathbf{OR} 7 THE ABILITY TO OPERATE OUTSIDE NORMAL TRUST **(V)** 8 BOUNDARIES WITH PRIVILEGED ACCESS. 9 "SUPPLY CHAIN RISK" MEANS A RISK THAT AN ADVERSARY MAY **(3)** SABOTAGE, MALICIOUSLY INTRODUCE UNWANTED FUNCTION TO, EXTRACT DATA 10 FROM, OR OTHERWISE SUBVERT THE DESIGN, INTEGRITY, MANUFACTURING, 11 12 PRODUCTION, DISTRIBUTION, INSTALLATION, OPERATION, MAINTENANCE, 13 DISPOSITION, OR RETIREMENT OF A SYSTEM OR ITEM OF SUPPLY SO AS TO SURVEIL, 14 DENY, DISRUPT, OR OTHERWISE MANIPULATE THE FUNCTION, USE, OR OPERATION OF THE SYSTEM OR ITEM OF SUPPLY OR INFORMATION STORED OR TRANSMITTED 15 BY OR THROUGH THE SYSTEM OR ITEM OF SUPPLY. 16 "ZERO-TRUST" MEANS A CYBERSECURITY APPROACH: 17 **(4) (I)** 18 FOCUSED ON CYBERSECURITY RESOURCE PROTECTION; 19 AND 20 BASED ON THE PREMISE THAT TRUST IS NEVER GRANTED (II) 21 IMPLICITLY BUT MUST BE CONTINUALLY EVALUATED. 22(b) This section does not apply to a public service company that is: 23(1) a common carrier; or **(2)** a telephone company. 24A public service company shall: 25(c) 26 adopt and implement cybersecurity standards that are equal to or (1) 27 exceed standards adopted by the Commission; 28adopt a zero-trust cybersecurity approach for on-premises services and (2)

1 establish minimum security standards for each operational technology 2 and information technology device based on the level of security risk for each device, 3 including [security risks associated with supply chains] SUPPLY CHAIN RISKS; and 4 on or before July 1, 2024, and on or before July 1 every other year **(4)** 5 thereafter, engage a third party to conduct an assessment of operational technology and 6 information technology devices THAT: 7 1. IS based on: 8 [1.] **A.** the Cybersecurity and Infrastructure Security 9 Agency's Cross-Sector Cybersecurity Performance Goals; or 10 **[2.] B.** a more stringent standard that is based on the 11 National Institute of Standards and Technology security frameworks; and 2. 12 ANALYZES CRITICAL SOFTWARE USED THE 13 OPERATIONAL TECHNOLOGY AND INFORMATION TECHNOLOGY DEVICES; AND 14 submit to the Commission AND THE OFFICE OF PEOPLE'S (ii) 15 COUNSEL certification of the public service company's compliance with standards used in 16 the assessments under item (i) of this item. 17 (d) Each public service company shall report, in accordance with the process established under paragraph (2) of this subsection, a cybersecurity incident, 18 19 including an attack on a system being used by the public service company, to the State 20 Security Operations Center in the Department of Information Technology. 21The State Chief Information Security Officer, in consultation with the (2)22Commission, shall establish a process for a public service company to report cybersecurity 23incidents under paragraph (1) of this subsection, including establishing: 24(i) the criteria for determining the circumstances under which a 25 cybersecurity incident must be reported; 26(ii) the manner in which a cybersecurity incident must be reported; 27 and 28 (iii) the time period within which a cybersecurity incident must be 29 reported.

The State Security Operations Center shall immediately notify

appropriate State and local agencies of a cybersecurity incident reported under this

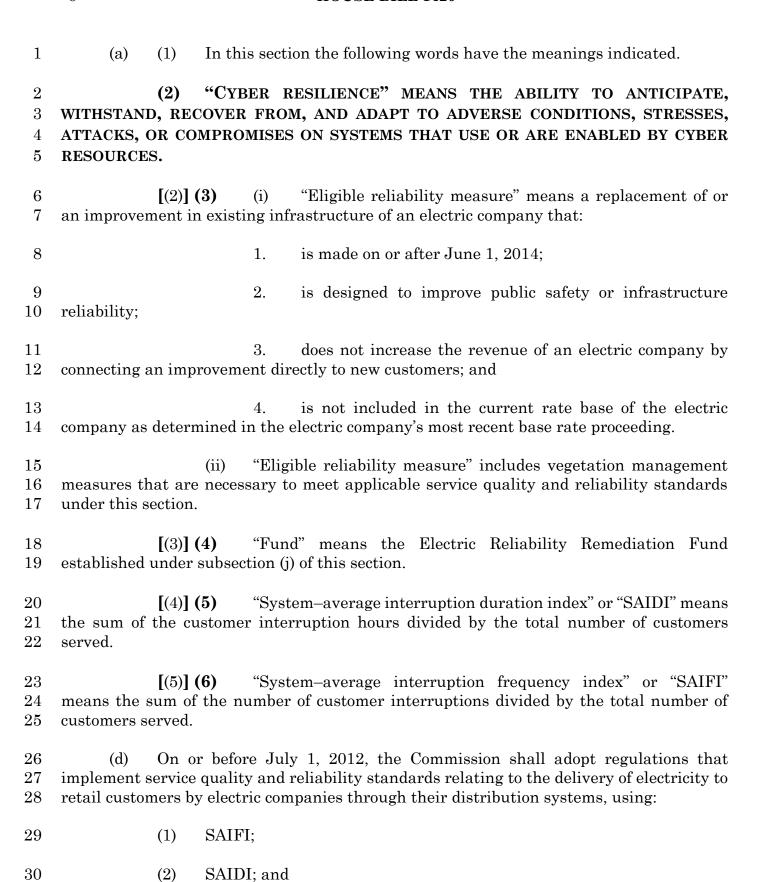
33 7–213.

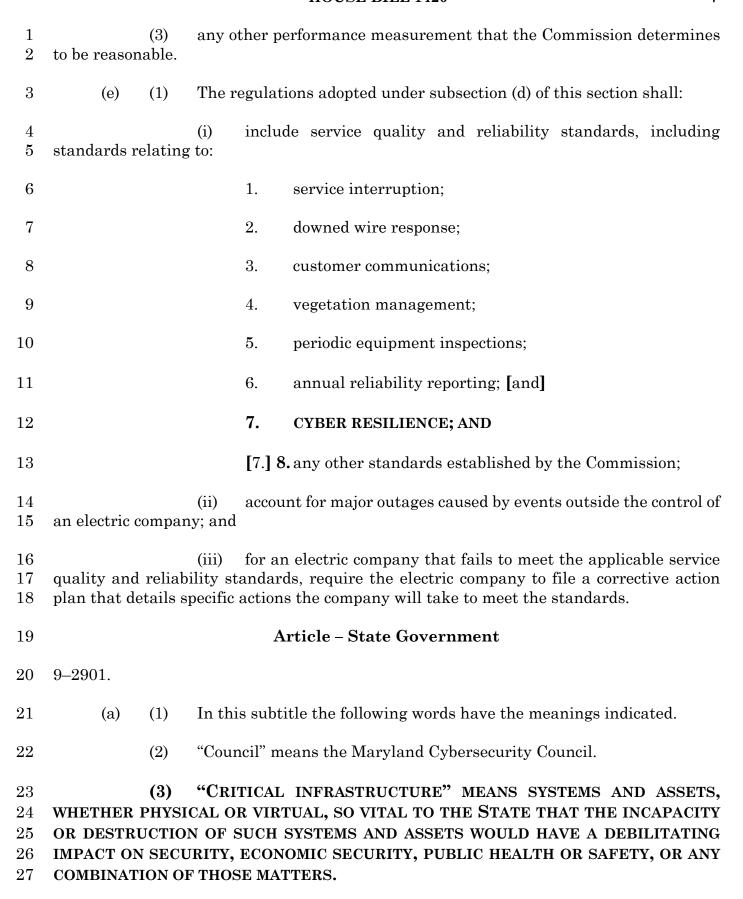
subsection.

(3)

30

31 32



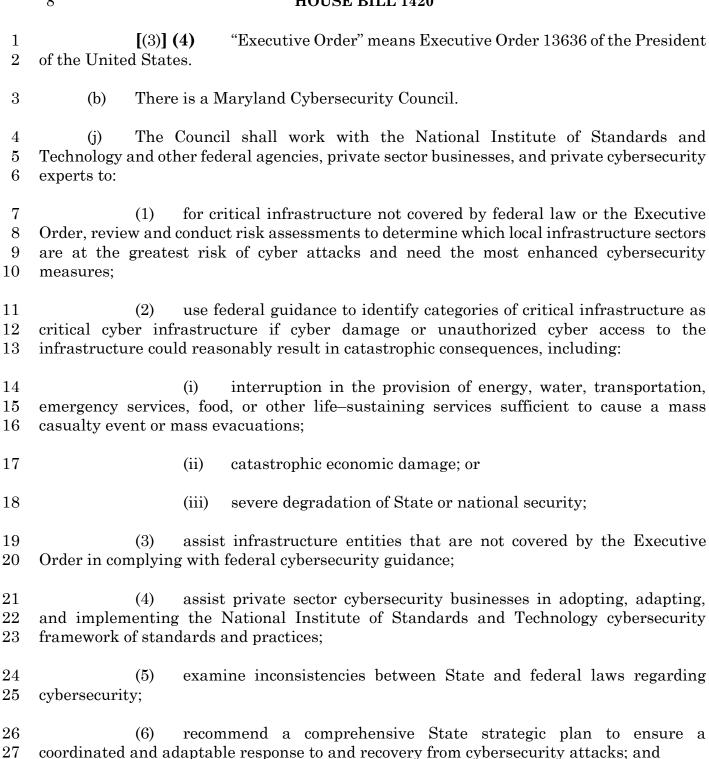


28

29

(7)

Council to address cybersecurity issues.



SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect 30 31 October 1, 2024.

recommend any legislative changes considered necessary by the