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 _____

AN ACT concerning

Cybersecurity – Office of People's Counsel, Public Service Companies, Public Service Commission, and Maryland Cybersecurity Council

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 perform certain duties~~ experts in the field of cybersecurity; requiring certain public service companies to engage with a third party to conduct an assessment that analyzes certain critical software; ~~requiring a certain certification to be submitted to the Office of People's Counsel;~~ requiring certain regulations adopted by the Public Service Commission to include cyber resilience; defining "critical infrastructure" for certain provisions relating to the Maryland Cybersecurity Council; and generally relating to cybersecurity.

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

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

EXPLANATION: **CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.**
[Brackets**]** indicate matter deleted from existing law.
Underlining indicates amendments to bill.
~~Strike out~~ indicates matter stricken from the bill by amendment or deleted from the law by amendment.

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

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

BY repealing and reenacting, without amendments,
Article – State Government
Section 9–2901(b) and (j)
Annotated Code of Maryland
(2021 Replacement Volume and 2023 Supplement)

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

Article – Public Utilities

2–203.

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

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

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

(3) CYBERSECURITY.

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

~~(2) The Office of People's Counsel shall hire:~~

~~**(I)** at least one assistant people's counsel who will focus on environmental issues; AND~~

~~(II) AT LEAST ONE ASSISTANT PEOPLE'S COUNSEL WITH CYBERSECURITY EXPERTISE TO:~~

~~1. ADVISE THE PEOPLE'S COUNSEL ON MEASURES TO IMPROVE OVERSIGHT OF THE CYBERSECURITY PRACTICES OF PUBLIC SERVICE COMPANIES;~~

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

~~3. ASSIST THE OFFICE OF PEOPLE'S COUNSEL IN MONITORING THE MINIMUM SECURITY STANDARDS DEVELOPED UNDER § 5–306 OF THIS ARTICLE;~~

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

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

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

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

5–306.

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

(1) focused on cybersecurity resource protection; and

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

(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:

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

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

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

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

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

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

(4) "ZERO–TRUST" MEANS A CYBERSECURITY APPROACH:

(I) FOCUSED ON CYBERSECURITY RESOURCE PROTECTION; AND

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

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

(1) a common carrier; or

(2) a telephone company.

(c) A public service company shall:

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

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

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

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

1. **IS** based on:

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

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

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

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

(d) (1) Each public service company shall report, in accordance with the process established under paragraph (2) of this subsection, a cybersecurity incident, including an attack on a system being used by the public service company, to the State Security Operations Center in the Department of Information Technology.

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

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

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

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

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

7–213.

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

(2) "CYBER RESILIENCE" MEANS THE ABILITY TO ANTICIPATE, WITHSTAND, RECOVER FROM, AND ADAPT TO ADVERSE CONDITIONS, STRESSES, ATTACKS, OR COMPROMISES ON SYSTEMS THAT USE OR ARE ENABLED BY CYBER RESOURCES.

[(2)**] (3)** (i) "Eligible reliability measure" means a replacement of or an improvement in existing infrastructure of an electric company that:

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

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

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

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

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

[(3)**] (4)** "Fund" means the Electric Reliability Remediation Fund established under subsection (j) of this section.

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

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

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

(1) SAIFI;

(2) SAIDI; and

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

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

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

1. service interruption;

2. downed wire response;

3. customer communications;

4. vegetation management;

5. periodic equipment inspections;

6. annual reliability reporting; **[**and**]**

7. CYBER RESILIENCE; AND

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

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

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

Article – State Government

9–2901.

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

(2) "Council" means the Maryland Cybersecurity Council.

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

[(3)**] (4)** "Executive Order" means Executive Order 13636 of the President of the United States.

(b) There is a Maryland Cybersecurity Council.

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

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

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

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

(ii) catastrophic economic damage; or

(iii) severe degradation of State or national security;

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

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

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

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

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

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