SENATE BILL 800

C5, S2 3lr1842
CF HB 969

By: **Senator Hester**
Introduced and read first time: February 6, 2023
Assigned to: Education, Energy, and the Environment

Committee Report: Favorable with amendments
Senate action: Adopted
Read second time: March 26, 2023

CHAPTER _____

AN ACT concerning

Public Service Commission – Cybersecurity Staffing and Assessments
(Critical Infrastructure Cybersecurity Act of 2023)

FOR the purpose of requiring the Public Service Commission to include on its staff a certain number of experts in cybersecurity to perform certain duties; requiring the Commission to establish, in coordination with the Office of Security Management, cybersecurity standards and best practices for regulated entities, share information on cybersecurity initiatives and best practices with certain entities, ~~and conduct a certain periodic assessment~~ collect certain certifications, and submit a certain report; requiring certain public service companies, including certain electric cooperatives, to adopt and implement certain cybersecurity standards and a zero–trust cybersecurity approach for certain services, establish certain minimum security standards, and periodically ~~contract~~ engage with a third party to conduct a certain assessment and submit certain information to the Commission beginning in a certain year; ~~requiring the Commission to conduct an evaluation on or before a certain date based on certain assessments;~~ requiring each public service company to report a cybersecurity incident to certain entities; requiring the State Chief Information Security Officer, in consultation with the Commission, to establish a certain reporting process; requiring the State Security Operations Center to immediately notify certain agencies of a cybersecurity incident reported under this Act; providing that, for a certain fiscal year, funds from the Dedicated Purpose Account may be transferred by budget amendment to the Department of Information Technology for a certain purpose; and generally relating to cybersecurity standards and assessments for public service companies and the Public Service Commission.

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 – Corporations and Associations
Section 5–637
Annotated Code of Maryland
(2014 Replacement Volume and 2022 Supplement)

BY repealing and reenacting, without amendments,
Article – Public Utilities
Section 1–101(a)
Annotated Code of Maryland
(2020 Replacement Volume and 2022 Supplement)

BY adding to
Article – Public Utilities
Section 1–101(h–1) and 5–306
Annotated Code of Maryland
(2020 Replacement Volume and 2022 Supplement)

BY repealing and reenacting, with amendments,
Article – Public Utilities
Section 2–108(d) and 2–113
Annotated Code of Maryland
(2020 Replacement Volume and 2022 Supplement)

BY repealing and reenacting, without amendments,
Article – State Finance and Procurement
Section 3.5–301(a) and (b)
Annotated Code of Maryland
(2021 Replacement Volume and 2022 Supplement)

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

Article – Corporations and Associations

5–637.

(a) (1) Except as provided in paragraph (2) of this subsection, this subtitle applies to the provision of broadband Internet service by a member–regulated cooperative.

(2) A member–regulated cooperative may not, for the sole purpose of providing broadband Internet service, exercise the power of condemnation under § 5–607(a)(16) of this subtitle.

(b) A member–regulated cooperative is subject to the following provisions of the Public Utilities Article:

(1) § 5–103;

(2) § 5–201;

(3) § 5–202;

(4) § 5–303;

(5) § 5–304;

(6) § 5–306;

[(6)**] (7)** § 7–103;

[(7)**] (8)** § 7–104;

[(8)**] (9)** § 7–203;

[(9)**] (10)** § 7–207;

[(10)**] (11)** § 7–302;

[(11)**] (12)** Title 7, Subtitle 5, Part I and Part II;

[(12)**] (13)** Title 7, Subtitle 7; and

[(13)**] (14)** § 13–101.

Article – Public Utilities

1–101.

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

(H–1) "CYBERSECURITY" HAS THE MEANING STATED IN § 3.5–301 OF THE STATE FINANCE AND PROCUREMENT ARTICLE.

2–108.

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

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

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

(3) **THE COMMISSION SHALL INCLUDE ON ITS STAFF ONE OR MORE EMPLOYEES THAT ARE EXPERTS IN CYBERSECURITY TO:**

(I) ADVISE THE CHAIRMAN OF THE COMMISSION AND THE COMMISSIONERS ON MEASURES TO IMPROVE OVERSIGHT OF THE CYBERSECURITY PRACTICES OF PUBLIC SERVICE COMPANIES;

(II) CONSULT WITH THE OFFICE OF SECURITY MANAGEMENT ON CYBERSECURITY ISSUES RELATED TO UTILITY REGULATION;

(III) ~~**STUDY AND MONITOR CYBERSECURITY BEST PRACTICES FOR INFORMATION TECHNOLOGY AND OPERATIONAL TECHNOLOGY;**~~

~~**(IV) ASSIST IN DRAFTING CYBERSECURITY–RELATED REGULATIONS;**~~

(V) ASSIST THE COMMISSION IN MONITORING THE MINIMUM SECURITY STANDARDS DEVELOPED UNDER § 5–306 OF THIS ARTICLE;

~~**(VI)**~~ **(IV) PARTICIPATE IN BRIEFINGS TO DISCUSS CYBERSECURITY PRACTICES BASED ON:**

1. APPLICABLE NATIONAL ASSOCIATION OF REGULATORY UTILITY COMMISSIONERS GUIDANCE; AND

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

(V) ~~**CONVENE WORKSHOPS WITH**~~ **SUPPORT PUBLIC SERVICE COMPANIES THAT DO NOT MEET MINIMUM SECURITY STANDARDS WITH REMEDIATING VULNERABILITIES OR ADDRESSING CYBERSECURITY ASSESSMENT FINDINGS**~~**; AND**~~**.**

~~**(VII) PREPARE REPORTS FOR THE COMMISSION TO REVIEW, INCLUDING REPORTS ON:**~~

~~1. CYBERSECURITY THREATS AND SOURCES; AND~~

~~2. THE EFFICACY OF CYBERSECURITY PRACTICES OF PUBLIC SERVICE COMPANIES.~~

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

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

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

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

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

(8) (I) THE COMMISSION SHALL:

~~(I)~~ 1. COLLABORATE WITH THE OFFICE OF SECURITY MANAGEMENT TO ESTABLISH CYBERSECURITY STANDARDS AND BEST PRACTICES FOR REGULATED ENTITIES, TAKING INTO ACCOUNT UTILITY NEEDS AND CAPABILITIES BASED ON SIZE;

~~(II)~~ 2. PERIODICALLY SHARE INFORMATION ON CYBERSECURITY INITIATIVES AND BEST PRACTICES WITH MUNICIPAL ELECTRIC UTILITIES; AND

~~(III)~~ 3. BEGINNING ON OR BEFORE ~~OCTOBER 1, 2023~~ JANUARY 1, 2025, AND EVERY 2 YEARS THEREAFTER~~;~~:

A. ~~EVALUATE~~ COLLECT CERTIFICATIONS OF A PUBLIC SERVICE COMPANY'S COMPLIANCE WITH STANDARDS USED IN THE ASSESSMENTS ~~SUBMITTED~~ CONDUCTED UNDER § 5–306 OF THIS ARTICLE FOR CYBERSECURITY–RELATED POLICIES AND PROCEDURES~~, INCLUDING CYBERSECURITY AND DATA PRIVACY THREAT PROTECTIONS~~; AND

**~~(IV)~~ B. SUBMIT ~~THE EVALUATION UNDER ITEM (III) OF THIS PARAGRAPH~~ A REPORT TO THE ~~OFFICE OF SECURITY MANAGEMENT IN THE~~

~~DEPARTMENT OF INFORMATION TECHNOLOGY AND THE MARYLAND DEPARTMENT OF EMERGENCY MANAGEMENT~~ **STATE CHIEF INFORMATION SECURITY OFFICER, OR THE OFFICER'S DESIGNEE.**

(II) THE REPORT REQUIRED UNDER SUBPARAGRAPH (I) OF THIS PARAGRAPH SHALL INCLUDE:

1. A GENERAL OVERVIEW OF CYBERSECURITY TECHNOLOGY AND POLICIES USED BY PUBLIC SERVICE COMPANIES IN THE STATE, GROUPED BY THE FOLLOWING TYPES:

A. INVESTOR–OWNED ELECTRIC COMPANIES;

B. ELECTRIC COOPERATIVES;

C. MUNICIPAL ELECTRIC COMPANIES;

D. GAS COMPANIES; AND

E. WATER COMPANIES;

2. GENERAL RECOMMENDATIONS FOR IMPROVING CYBERSECURITY TECHNOLOGY AND POLICIES USED BY PUBLIC SERVICE COMPANIES IN THE STATE, GROUPED BY THE FOLLOWING TYPES:

A. INVESTOR–OWNED ELECTRIC COMPANIES;

B. ELECTRIC COOPERATIVES;

C. MUNICIPAL ELECTRIC COMPANIES;

D. GAS COMPANIES; AND

E. WATER COMPANIES; AND

3. FOR EACH CERTIFICATION COLLECTED:

A. THE NAME OF THE PUBLIC SERVICE COMPANY;

B. THE DATE OF THE PUBLIC SERVICE COMPANY'S MOST RECENT CYBERSECURITY ASSESSMENT;

C. THE CYBERSECURITY FRAMEWORK USED IN THE CYBERSECURITY ASSESSMENT OF THE PUBLIC SERVICE COMPANY; AND

D. THE NAME OF THE ENTITY THAT COMPLETED THE CYBERSECURITY ASSESSMENT.

[(7)**] (9)** Subject to § 3–104 of this article, the Commission may delegate to a commissioner or personnel the authority to perform an administrative function necessary to carry out a duty of the Commission.

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

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

1. each commissioner of the Commission;

2. the Executive Director;

3. the General Counsel and each assistant general counsel;

4. the Executive Secretary;

5. the commissioners' personal staff members;

6. the chief public utility law judge; and

7. each license hearing officer.

2–113.

(a) (1) The Commission shall:

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

1. ensure their operation in the interest of the public; and

2. promote adequate, economical, and efficient delivery of utility services in the State without unjust discrimination; and

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

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

(i) the public safety;

(ii) the economy of the State;

(iii) the maintenance of fair and stable labor standards for affected workers;

(iv) the conservation of natural resources;

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

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

(VII) THE PROTECTION OF A PUBLIC SERVICE COMPANY'S INFRASTRUCTURE AGAINST CYBERSECURITY THREATS.

(b) The powers and duties listed in this title do not limit the scope of the general powers and duties of the Commission provided for by this division.

5–306.

(A) 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.

(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; AND

(4) (I) ~~BEGINNING IN 2024~~ ON OR BEFORE JULY 1, 2024, AND ~~AT LEAST ONCE~~ ON OR BEFORE JULY 1 EVERY OTHER YEAR THEREAFTER, ~~CONTRACT WITH~~ ENGAGE A THIRD PARTY TO CONDUCT AN ASSESSMENT OF OPERATIONAL TECHNOLOGY AND INFORMATION TECHNOLOGY DEVICES BASED ON:

1. THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY'S CROSS–SECTOR CYBERSECURITY PERFORMANCE GOALS; OR

2. A MORE STRINGENT STANDARD THAT IS BASED ON THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY SECURITY FRAMEWORKS; AND

(II) SUBMIT TO THE COMMISSION:

~~1. THE RESULTS AND RECOMMENDATIONS OF EACH ASSESSMENT; AND~~

~~2.~~ 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.

Article – State Finance and Procurement

3.5–301.

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

(b) "Cybersecurity" means processes or capabilities wherein systems, communications, and information are protected and defended against damage, unauthorized use or modification, and exploitation.

SECTION 2. AND BE IT FURTHER ENACTED, That~~, on or before October 1, 2024, the Public Service Commission shall conduct an evaluation based on assessments conducted on a public service company's information technology devices conducted under Section 1 of this Act~~ for fiscal year 2024, funds from the Dedicated Purpose Account may be transferred by budget amendment, in accordance with § 7–310 of the State Finance and Procurement Article, to the Department of Information Technology for the purpose of adding additional staffing and operational capacity for the Department to improve State and local cybersecurity.

SECTION 3. AND BE IT FURTHER ENACTED, That it is the intent of the General Assembly that the Public Service Commission work with the Cybersecurity and Infrastructure Security Agency and the Office of Security Management to improve the Commission's capacity to implement the provisions of this Act.

SECTION 4. AND BE IT FURTHER ENACTED, That this Act shall take effect ~~October~~ July 1, 2023.