By: Delegate Kerr
Introduced and read first time: February 11, 2022
Assigned to: Economic Matters

A BILL ENTITLED

AN ACT concerning

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

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

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

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

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

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.
[Brackets] indicate matter deleted from existing law.
BY adding to
Article – Public Utilities
Section 1–101(h–1) through (h–3) and 5–305
Annotated Code of Maryland
(2020 Replacement Volume and 2021 Supplement)

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

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

Article – Public Safety

14–101.

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

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

(1) SECURITY;

(2) ECONOMIC SECURITY;

(3) PUBLIC HEALTH; OR

(4) PUBLIC SAFETY.

(C) (1) “CYBERSECURITY” MEANS PROCESSES OR CAPABILITIES IN
WHICH SYSTEMS, COMMUNICATIONS, AND INFORMATION ARE PROTECTED AND
DEFENDED AGAINST DAMAGE, UNAUTHORIZED USE OR MODIFICATION, AND
EXPLOITATION.

(2) “CYBERSECURITY” INCLUDES PROTECTING THE AVAILABILITY,
INTEGRITY, AUTHENTICATION, CONFIDENTIALITY, AND NONREPUDIATION OF
INFORMATION.

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

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

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

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

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

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

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

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

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

(1) the mayor;

(2) the county executive;

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

(4) for a municipal corporation that does not have a mayor, the burgess, chairperson, or president of the municipal governing body or other chief executive officer of the municipal corporation.
(a) To ensure that the State will be adequately prepared to deal with emergencies, to protect the public peace, health, and safety in the State, to preserve the lives and property of the people of the State, and to ensure the social and economic resilience of the State, it is necessary to:

(1) establish a Maryland Department of Emergency Management;

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

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

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

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

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

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

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

(c) The Department may act to:

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

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

(3) coordinate emergency management activities and operations:

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

(ii) between State agencies and political subdivisions;

(iii) with local governments;

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

(v) with private and nonprofit entities.

14–118.

(A) IN THIS SECTION, “PROGRAM” MEANS THE CRITICAL INFRASTRUCTURE CYBERSECURITY GRANT PROGRAM.

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

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

(D) THE DEPARTMENT SHALL:

(1) ADMINISTER THE PROGRAM;

(2) ESTABLISH APPLICATION PROCEDURES FOR THE PROGRAM; AND

(3) AWARD GRANTS FROM THE PROGRAM.

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

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

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

2. PREPARE A REPORT ON THE CYBERSECURITY RISKS IDENTIFIED UNDER ITEM 1 OF THIS ITEM;
(II) IDENTIFY FUNDING TO FUND THE GRANTS AWARDED UNDER THE PROGRAM; AND

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

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

(F) THE DEPARTMENT SHALL:

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

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

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

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

Article – Public Utilities

1–101.

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

(H–1) “CYBER RESILIENCY” 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 A CYBER RESOURCE.

(H–2) “CYBER RESOURCE” MEANS AN INFORMATION SOURCE THAT:

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

(2) CAN BE ACCESSED BY A NETWORK OR BY USING NETWORKING
METHODS.

(H–3) “Cybersecurity” has the meaning stated in § 14–101 of the Public Safety 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 dedicated to cybersecurity policy, strategy, auditing, and reporting.

(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.

[(7)] (8) 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.
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.

(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 CYBERSECURITY RISKS FACED BY PUBLIC SERVICE COMPANIES IN THE STATE.

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.

5–305.

(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) EACH PUBLIC SERVICE COMPANY SHALL:
HOUSE BILL 1339

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

2. (2) PROTECT PERSONALLY IDENTIFIABLE INFORMATION OF CUSTOMERS AND EMPLOYEES;

3. (3) INCLUDE IN CONTRACTS WITH THIRD–PARTY INFORMATION TECHNOLOGY OR OPERATIONAL TECHNOLOGY PROVIDERS PROVISIONS REQUIRING THE THIRD–PARTY PROVIDERS TO:

   (i) COLLECT AND PRESERVE DATA FOR CYBERSECURITY ANALYSIS; AND

   (ii) SHARE THAT DATA AND REPORT ANY CYBERSECURITY BREACHES TO THE PUBLIC SERVICE COMPANY;

4. (4) ESTABLISH MINIMUM SECURITY STANDARDS FOR INFORMATION TECHNOLOGY AND OPERATIONAL TECHNOLOGY DEVICES; AND

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

7–213.

(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. (1) SAIFI;

2. (2) SAIDI; and

3. (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 RESILIENCY; AND
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.

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

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