HB4725

LRB10222900SPS32053b

102ND GENERAL ASSEMBLY

State of Illinois

2021 and 2022

HB4725

Introduced 1/27/2022, by Rep. Bob Morgan

SYNOPSIS AS INTRODUCED:

220 ILCS 5/4-101 from Ch. 111 2/3, par. 4-101
220 ILCS 5/4-102 new

Amends the Public Utilities Act. Provides that all public utilities are required to establish a security policy. Provides that Illinois Commerce Commission staff shall determine entities subject to the attestation and reporting requirements. Provides that each entity subject to the attestation and reporting requirements shall provide to the Commission, by July 31 of each year, an annual affidavit signed by a senior executive responsible for security of the regulated entity that states the entity has a security policy that satisfies specified requirements. Provides that the entity shall also, at least annually, provide to the Commission a report on the entity's cybersecurity program and related information. Provides that entities subject to this shall inform the Commission, in a written or oral report, within 48 hours or as soon as practicable, after the discovery or occurrence of any notable, unusual, or significant cybersecurity incident. Provides that attestations, reports, and other submissions made shall not be open to public inspection unless otherwise ordered by the Commission.

LRB102 22900 SPS 32053 b

A BILL FOR

AN ACT concerning regulation.

Be it enacted by the People of the State of Illinois, represented in the General Assembly:

Section 5. The Public Utilities Act is amended by changing Section 4-101 and by adding Section 4-102 as follows:

(220 ILCS 5/4-101) (from Ch. 111 2/3, par. 4-101)

Sec. 4-101. The Commerce Commission shall have general supervision of all public utilities, except as otherwise provided in this Act, shall inquire into the management of the business thereof and shall keep itself informed as to the manner and method in which the business is conducted. It shall examine those public utilities and keep informed as to their general condition, their franchises, capitalization, rates and other charges, and the manner in which their plants, equipment and other property owned, leased, controlled or operated are managed, conducted and operated, not only with respect to the adequacy, security and accommodation afforded by their service but also with respect to their compliance with this Act and any other law, with the orders of the Commission and with the charter and franchise requirements.

Whenever the Commission is authorized or required by law to consider some aspect of criminal history record information for the purpose of carrying out its statutory powers and

responsibilities, then, upon request and payment of fees in conformance with the requirements of Section 2605-400 of the Illinois State Police Law, the Illinois State Police is authorized to furnish, pursuant to positive identification, such information contained in State files as is necessary to fulfill the request.

~~The Commission shall require all public utilities to establish a security policy that includes on site safeguards to restrict physical or electronic access to critical infrastructure and computerized control and data systems. The Commission shall maintain a record of and each regulated entity shall provide to the Commission an annual affidavit signed by a representative of the regulated entity that states:~~

~~(1) that the entity has a security policy in place;~~

~~(2) that the entity has conducted at least one practice exercise based on the security policy within the 12 months immediately preceding the date of the affidavit; and~~

~~(3) with respect to any entity that is an electric public utility, that the entity follows, at a minimum, the most current security standards set forth by the North American Electric Reliability Council.~~

(Source: P.A. 102-538, eff. 8-20-21.)

(220 ILCS 5/4-102 new)

Sec. 4-102. Security policy.

(a) The Commission shall require public utilities to establish a security policy in order to:

(1) gather sufficient information regarding entities that affect large numbers of Illinois population while balancing any administrative burden on Commission staff and regulated entities;

(2) gather sufficient depth of information regarding security policies, implementations, and incidents while avoiding the creation of a repository of valuable sensitive information residing in the Commission's electronic and physical systems that may lead to undesirable disclosure of critical infrastructure information through legal, procedural, or technical means, and making the Commission a target for attackers; and

(3) encourage regulated entities to go beyond minimum security requirements and use a risk-based approach to apply the most effective interventions in the ever-evolving threat landscape.

(b) All public utilities are required to establish a security policy. Commission staff shall, at the direction and discretion of the Executive Director, determine entities subject to the attestation and reporting requirements in this Section.

(c) Each entity subject to the attestation and reporting requirements of this Section, as identified in subsection (b),

shall provide to the Commission, by July 31 of each year, submitted through electronic filing or as otherwise directed by the Executive Director or designated Commission staff, and the Commission shall maintain a record of, an annual affidavit signed by a senior executive responsible for security of the regulated entity that states the entity has a security policy in place that:

(1) includes, but is not limited to, safeguards to restrict physical and electronic access to critical infrastructure and computerized control and data systems;

(2) is documented in electronic or paper format;

(3) is updated at least annually;

(4) includes at least one practice exercise based on the security policy within the 12 months immediately preceding the date of the affidavit;

(5) follows industry best practices and is based on widely-accepted frameworks and standards, and

(A) with respect to any entity that is an electric public utility, that the entity follows, at a minimum, the most current security standards set forth by the North American Electric Reliability Corporation;

(B) with respect to any entity that is a gas public utility, that the entity follows, at a minimum, the most current security standards or guidelines set forth by the Transportation Security Agency; and

(C) with respect to any entity that is a water

public utility, that the entity follows, at a minimum, the most current security standards or guidelines set forth by the American Water Works Association and recognized by the federal Environmental Protection Agency;

(6) is appropriate for the entity's risk profile and potential threats as identified in regular risk assessments;

(7) requires implementation of risk management strategies;

(8) has been assessed by a third-party at least every 2 years for its implementation;

(9) has a program for addressing vulnerabilities found through assessments;

(10) documents key contact information of other entities with whom the regulated entity maintains partnerships for information sharing, planning, and situational awareness;

(11) manages security risks from both intentional and unintentional insider actions;

(12) manages security risks from vendors throughout the supply chain; and

(13) contemplates cybersecurity insurance, whether or not the entity acquires or maintains cybersecurity insurance.

(d) In addition to the annual attestations that the

regulated entity's security policy contains the components in subsection (c), the regulated entity shall also, at least annually, provide a written or oral annual report, individually or jointly with other regulated entities, to the Executive Director or designated Commission staff regarding the regulated entity's cybersecurity program and related information. This report shall include, but is not limited to, the following information:

(1) an overview of the regulated entity's approach to cybersecurity awareness and protection, including all items listed in the attestation;

(2) a description of cybersecurity awareness training efforts for the regulated entity's staff members, specialized cybersecurity training for cybersecurity personnel, and participation by the regulated entity's cybersecurity staff in emergency preparedness exercises in the previous calendar year;

(3) an organizational diagram of the regulated entity's cybersecurity organization, including positions and contact information for primary and secondary cybersecurity emergency contacts;

(4) a description of the regulated entity's internal and external communications plan regarding unauthorized actions that result in interruption, degradation of service, financial harm, or breach of sensitive business or customer data, including the regulated entity's plan

for notifying the Commission and customers;

(5) a redacted summary of any unauthorized actions that resulted in material interruption, financial harm, or breach of sensitive business or customer data, including the parties that were notified of the unauthorized action and any remedial actions undertaken;

(6) key performance indicators and other metrics related to physical security and cybersecurity;

(7) any notable cybersecurity information not included in paragraphs (1) through (6); and

(8) any other information as directed by the Executive Director or designated Commission staff.

(e) Regulated entities subject to this Section shall inform the Commission, in a written or oral report, within 48 hours or as soon as practicable, after the discovery or occurrence of any notable, unusual, or significant cybersecurity incident, or any cybersecurity incident that must be reported to another regulatory agency, or as directed by designated Commission staff, unless otherwise prohibited by law or court order or instructed otherwise by law enforcement personnel.

(f) Regulated entities subject to this Section shall make the relevant security policy, assessments, reports, and related documents available for review by designated Commission staff.

(g) Attestations, reports, and other submissions made

under this Section shall not be open to public inspection unless otherwise ordered by the Commission. Regulated entities shall not report information otherwise required under this Section if prohibited by law or court order or instructed otherwise by law enforcement personnel.

(h) The Commission may adopt rules to implement this Section.