HB3576

LRB10408875AAS18930b

104TH GENERAL ASSEMBLY

State of Illinois

2025 and 2026

HB3576

Introduced 2/18/2025, by Rep. Dagmara Avelar

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, within 120 days after the effective date of the amendatory provisions, each water purveyor shall develop a cybersecurity program that defines and implements organizational accountabilities and responsibilities for cyber risk management activities, and establishes policies, plans, processes, and procedures for identifying and mitigating cyber risk to its public community water system. Provides that, within certain time periods after the effective date of the amendatory provisions, a water purveyor shall create a cybersecurity incident reporting process; obtain a cybersecurity insurance policy that meets certain standards; reasonably conform to the most recent version of one or more of specified industry-recognized cybersecurity frameworks; submit a compliance report; submit an incident report; and submit an annual status report. Sets forth provisions concerning violations of the amendatory provisions and rulemaking abilities of the Department of Natural Resources and the Illinois Commerce Commission. Makes other changes.

LRB104 08875 AAS 18930 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.

A water public utility's security policy shall also meet the requirements set forth in Section 4-102.

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

(220 ILCS 5/4-102 new)

Sec. 4-102. Cybersecurity policy for water purveyors.

(a) As used in this Section:

"Cybersecurity incident" means an event occurring on or conducted through a computer network that jeopardizes the integrity, confidentiality, or availability of computers, information systems, communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information residing on such computers or information systems.

"Cybersecurity insurance policy" means an insurance policy designed to mitigate losses from cybersecurity incidents, including, but not limited to, data breaches, business interruption, and network damage.

"Department" means the Department of Natural Resources.

"Industrial control system" means an information system used to control industrial processes such as manufacturing, product handling, production, or distribution.

"Industrial control system" includes supervisory control and data acquisition systems used to control geographically dispersed assets, and distributed control systems and smaller control systems using programmable logic controllers to control localized processes.

"Information resource" means information and related resources, such as personnel, equipment, funds, and

information technology.

"Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

"Public community water system" means a public water system which serves at least 15 service connections used by year-round residents or regularly serves at least 25 year-round residents.

"Public water system" means a system for the provision to the public of water for human consumption through pipes or other constructed conveyances, if such system has at least 15 service connections or regularly serves an average of at least 25 individuals daily at least 60 days out of the year. "Public water system" includes (i) any collection, treatment, storage and distribution facilities under control of the operator of such system and used primarily in connection with such system, and (ii) any collection or pre-treatment storage facilities not under such control which are used primarily in connection with such system.

"Water purveyor" means any person that owns a public community water system with more than 500 service connections.

(b) Within 120 days after the effective date of this amendatory Act of the 104th General Assembly, each water purveyor shall develop a cybersecurity program that defines and implements organizational accountabilities and

responsibilities for cyber risk management activities, and establishes policies, plans, processes, and procedures for identifying and mitigating cyber risk to the water purveyor's public community water system. As part of the cybersecurity program, a water purveyor shall do the following:

(1) identify the individual directly responsible for ensuring that the policies, plans, processes, and procedures established pursuant to this Section are executed in a timely manner;

(2) conduct risk assessments and implement appropriate controls to mitigate identified risks to the public community water system;

(3) maintain situational awareness of cyber threats and vulnerabilities to the public community water system; and

(4) create and exercise incident response and recovery plans.

A water purveyor shall submit a copy of the cybersecurity program developed pursuant to this subsection (b) to the Commission in a form and manner as determined by the Commission.

(c) Within 60 days after developing the cybersecurity program required pursuant to subsection (b) of this Section, each water purveyor shall create a cybersecurity incident reporting process.

(d) No later than 180 days after the effective date of this

amendatory Act of the 104th General Assembly, each water purveyor shall obtain a cybersecurity insurance policy that meets any applicable standards adopted by the Commission.

(e) No later than 180 days after the effective date of this amendatory Act of the 104th General Assembly, each water purveyor shall update its cybersecurity program developed pursuant to this Section to apply to all of the public community water system's industrial control systems and to reasonably conform to the most recent version of one or more of the following industry-recognized cybersecurity frameworks:

(1) the Framework for Improving Critical Infrastructure Cybersecurity developed by the National Institute of Standards and Technology;

(2) the Center for Internet Security Critical Security Controls for Effective Cyber Defense; or

(3) the International Organization for Standardization and International Electrotechnical Commission 27000 family of standards for an information security management system.

Whenever a final revision to one or more of the frameworks listed in this subsection (e) is published, a water purveyor whose cybersecurity program conformed to that framework shall revise its cybersecurity program to reasonably conform to the revised framework, and submit a copy of the revised cybersecurity program to the Commission, no later than 180 days after publication of the revised framework.

(f) No later than one year after the effective date of this amendatory Act of the 104th General Assembly, and each year thereafter, each water purveyor shall submit to the Department and the Commission a certification demonstrating that the water purveyor is in compliance with the requirements of this Section. The certification shall be made in a form and manner as determined by the Department, in consultation with the Commission. The certification shall be signed by a senior executive responsible for security of the regulated entity.

(g) The Commission shall cause to be audited any public community water system that fails to submit a cybersecurity program, a revision, or a certification pursuant to this Section. Any audit shall be conducted by a qualified and independent cybersecurity company, at the water purveyor's expense. Following the audit, the water purveyor shall submit the audit and any corrective action plans derived from the audit to the Commission.

(h) A water purveyor shall, upon the request of the Department or the Commission, provide proof of compliance with the requirements of this Section, in a form and manner as determined by the Department or by the Commission.

(i) On and after 90 days after the effective date of this amendatory Act of the 104th General Assembly, a water purveyor 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, including the following:

(1) any cybersecurity incident that results in the compromise of the confidentiality, integrity, availability, or privacy of the water purveyor's utility billing, communications, data management, or business information systems, or the information on such systems; and

(2) any cybersecurity incident against the water purveyor's industrial control systems, including monitoring, operations, and centralized control systems, that adversely impacts, disables, or manipulates infrastructure, resulting in loss of service, contamination of finished water, or damage to infrastructure.

(j) No later than 30 days after receiving a report of a cybersecurity incident from a water purveyor pursuant to subsection (i), the Commission shall cause to be audited the water purveyor's cybersecurity program and any actions the water purveyor took in response to the cybersecurity incident. The audit shall identify cyber threats and vulnerabilities to the public community water system, weaknesses in the public community water system's cybersecurity program, and strategies to address those weaknesses so as to protect the public community water system from the threat of future cybersecurity

incidents. Any audit shall be conducted by a qualified and independent cybersecurity company at the water purveyor's expense. After the completion of the audit, the water purveyor shall submit the audit and any corrective action plans derived from the audit to the Commission.

(k) By July 31 of each year, a water purveyor shall provide to the Commission a report that identifies the following:

(1) an overview of the water purveyor's approach to cybersecurity awareness and protection;

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

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

(4) a description of the water purveyor'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 water purveyor'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 Commission.

(l) The Department or the Commission shall create a centralized portal allowing for electronic submittal of the report required under this Section. The lack of a centralized portal pursuant to this subsection (l) shall not negate the requirement for a water purveyor to submit a report.

(m) Any person who violates the provisions of this Section, or any rule or regulation adopted pursuant thereto, shall be subject to the penalties and other remedies set forth in Sections 4-202 and Section 4-203. No later than 18 months after the effective date of this amendatory Act of the 104th General Assembly, the Department shall adopt a schedule of civil administrative penalties for specific violations of this Section.

(n) 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.

(o) The Department or the Commission may adopt rules to implement this Section.