By Senator Hutson

7-00350-22 2022828__

A bill to be entitled

An act relating to critical infrastructure; providing a short title; creating s. 943.6873, F.S.; providing legislative findings; defining terms; requiring that, beginning on a specified date, asset owners ensure that the operation and maintenance of operational technology comply with specified standards and practices; requiring, beginning on a specified date, asset owners to require that certain components, services, and solutions conform to such standards and practices; requiring that certain contracts for critical infrastructure meet specified minimum standards; providing requirements and procedures relating to civil actions based on cybersecurity-breach-related claims; authorizing a court to take specified action upon a showing that a business, a service provider, or another person or entity violates the act; authorizing the Department of Law Enforcement to institute appropriate legal proceedings against a business, a service provider, or another person or entity that violates the act; providing procedures for such legal proceedings; providing for departmental actions; requiring the department to adopt rules; providing an effective date.

WHEREAS, the operational technologies that automate the critical infrastructure of and commercial facilities in this state are experiencing a rapid increase in cybersecurity incidents, and the impact is serious, affecting daily life,

public safety, the environment, and economic viability across sectors, and

WHEREAS, the recent cybersecurity intrusion of the public water system in Oldsmar, the hacking and shutdown of the Colonial Pipeline by the criminal enterprise Darkside, the infiltration of the Bowman Dam in Rye Brook, New York, by Iranian hackers in 2013, and the intrusion of numerous federal agencies by suspected Russian hackers underscore the need to provide the public and private sectors with clarity and support in improving control systems cybersecurity, NOW, THEREFORE,

Be It Enacted by the Legislature of the State of Florida:

Section 1. This act may be cited as the "Critical Infrastructure Standards and Procedures Act."

Section 2. Section 943.6873, Florida Statutes, is created to read:

943.6873 Critical infrastructure standards; civil actions.—

(1) The Legislature finds that a standard definition of the security capabilities for system components will provide a common language for product suppliers and all other control system stakeholders, simplifying the procurement and integration processes for the computers, applications, network equipment, and control devices that make up a control system. The United States National Institute of Standards and Technology (NIST) published the NIST Cybersecurity Framework, which references several relevant cybersecurity standards, including the internationally recognized ISA/IEC 62443 series of standards. These standards define a set of measures and benchmarks

specifically built to guide organizations through the process of assessing the risk associated with a particular automation and control system and in identifying and applying security countermeasures to reduce that risk.

(2) As used in this section, the term:

(a) "Asset owner" means the public or private owner of, or the entity accountable and responsible for operation of, the critical infrastructure and the automation and control system. The asset owner is also the operator of the automation and control system components and the equipment under its control.

(b) "Automation and control system" means a collection of personnel, hardware, software, and policies associated with the operation of the critical infrastructure which can affect or influence its safe, secure, and reliable operation.

(c) "Automation and control system component" means control systems and any complementary hardware and software components installed and configured to operate in an automation and control system. These systems include, but are not limited to:

1. Control systems, including distributed control systems, programmable logic controllers, remote terminal units, intelligent electronic devices, supervisory control and data acquisition, networked electronic sensing and control, monitoring and diagnostic systems, and process control systems that include physically separate or integrated basic process control system and safety-instrumented system functions;

2. Associated information systems, such as advanced or multivariable control, online optimizers, dedicated equipment monitors, graphical interfaces, process historians, manufacturing execution systems, and plant information

management systems; and

3. Associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes as defined by the International Society of Automation ISA/IEC 62443 series of standards as referenced by the NIST Cybersecurity Framework.

(d) "Critical infrastructure" means all physical and virtual assets, systems, and networks considered vital and vulnerable to cybersecurity attacks, as determined by the department in consultation with the Florida Digital Service and the Florida Cybersecurity Advisory Council. Critical infrastructure includes, but is not limited to, public transportation as defined in s. 163.566; water and wastewater treatment facilities, public utilities, and public services subject to the jurisdiction, supervision, powers, and duties of the Florida Public Service Commission; public buildings, including those operated by the State University System; hospitals and public health facilities; and financial services organizations regulated by the Department of Financial Services.

(e) "Cybersecurity-breach-related claim" means a legal proceeding or civil action against an asset owner for failure to meet the minimum standards required by this section.

(f) "Department" means the Department of Law Enforcement.

(g) "Operation technology" means the hardware and software that detects or causes a change through the direct monitoring or control of physical devices and systems, processes, and events in the critical infrastructure.

(3) Beginning on July 1, 2024, the asset owner shall ensure

that the operation and maintenance of operational technology, including critical infrastructure, automation control systems, and automation control system components, are compliant with the standards and practices defined in the ISA/IEC 62443 series of standards as referenced by the NIST Cybersecurity Framework, including annual risk assessments and creation of a mitigation plan.

(4) Beginning on July 1, 2026, when procuring automation and control system components, services, or solutions, or when contracting for facility upgrades or the construction of critical infrastructure facilities, an asset owner shall require that those components, services, or solutions conform to the ISA/IEC 62443 series of standards as referenced by the NIST Cybersecurity Framework for defining measures to assure conformance. All contracts awarded for construction, reconstruction, alteration, design, or commissioning of facilities identified as critical infrastructure must require that installed automation and control components meet the minimum standards for cybersecurity as defined by the ISA/IEC 62443 series of standards as referenced by the NIST Cybersecurity Framework.

(5) In any civil action based on a cybersecurity-breach-related claim, including a civil action brought by the department pursuant to subsection (6):

(a) A court shall determine as a matter of law whether the defendant made a good faith effort to comply with subsection (3) or subsection (4), as applicable.

(b) If the court determines that the defendant made such a good faith effort, the defendant is immune from civil liability.

(c) If the court determines that the defendant did not make such a good faith effort, the plaintiff may proceed with the action.

(d) The trial court, upon a showing that any business, service provider, or other person or entity is in violation of this section, may take any of the following actions:

1. Issue a temporary or permanent injunction.

2. Impose a civil penalty of not more than $2,500 for each unintentional violation or $7,500 for each intentional violation.

3. Award reasonable costs of enforcement, including reasonable attorney fees and costs.

4. Grant any other relief as the court deems appropriate.

(6) If the department has reason to believe that any business, service provider, or other person or entity is in violation of this section and that proceedings would be in the public interest, the department may institute an appropriate legal proceeding, which may include a civil action, against such party.

(a) After the department has notified a business in writing of an alleged violation, the department may grant the business, service provider, or other person or entity a 30-day period to cure the alleged violation. The department may consider the number of violations, the substantial likelihood of injury to the public, or the safety of persons or property in determining whether to grant the 30-day period to cure an alleged violation.

(b) If the business, service provider, or other person or entity cures the alleged violation to the satisfaction of the department and provides proof of such cure to the department,

the department may issue a letter of guidance to the business, service provider, or other person or entity which indicates that the business, service provider, or other person or entity will not be offered a 30-day cure period for any future violation. If the business, service provider, or other person or entity fails to cure the violation within 30 days, the department may bring a legal proceeding against the business for the alleged violation.

(7) The department shall adopt rules, in consultation with the Florida Digital Service and the Florida Cybersecurity Advisory Council, to implement and administer this section.

Section 3. This act shall take effect October 1, 2022.