By the Committee on Governmental Oversight and Accountability; and Senator Hutson

585-02668-22 2022828c1

A bill to be entitled

An act relating to critical infrastructure standards and procedures; creating s. 282.32, F.S.; providing a short title; providing legislative findings; providing definitions; requiring a local government asset owner procuring certain components, services, or solutions or entering into certain contracts to require conformance with certain standards, beginning on a specified date; requiring such a local government asset owner to ensure that certain contracts require that certain components meet certain minimum standards; requiring the Florida Digital Service, in consultation with the Florida Cybersecurity Advisory Council, to adopt rules; providing an effective date.

WHEREAS, the operational technologies that automate the critical infrastructure of daily life are experiencing a rapid increase in cybersecurity incidents, and the impact of such incidents affect life, safety, the environment, and economic viability across sectors, and

WHEREAS, the recent cybersecurity hacking and shutdown of the Colonial Pipeline by the criminal enterprise DarkSide in 2021; the infiltration of the Bowman Avenue 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 on how to improve the cybersecurity of control systems, NOW, THEREFORE, Be It Enacted by the Legislature of the State of Florida:

Section 1. Section 282.32, Florida Statutes, is created to read:

282.32 Critical infrastructure standards and procedures.—

(1) This section may be cited as the "Critical Infrastructure Standards and Procedures Act."

(2) The Legislature finds that standard definitions of the security capabilities of system components are necessary to provide a common language for product suppliers and other control system stakeholders and to simplify 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 Cybersecurity Framework (NIST CSF), which references several relevant cybersecurity standards, including the International Society of Automation ISA 62443 series of standards, is an appropriate resource for use in establishing such standard definitions.

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

(a) "Automation and control system" means the personnel, hardware, software, and policies involved in the operation of critical infrastructure which may affect or influence such critical infrastructure's safe, secure, and reliable operation.

(b) "Automation and control system component" means control systems and complementary hardware and software components that are installed and configured to operate in an automation and control system. For purposes of this section, the term "control systems" includes, but is not limited to:

1. 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, including basic process control system and safety-instrumented system functions, regardless of whether such functions are physically separate or integrated.

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

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 in the ISA 62443 series of standards as referenced by the NIST CSF.

(c) “Critical infrastructure” means infrastructure for which all assets, systems, and networks, regardless of whether physical or virtual, are considered vital and vulnerable to cybersecurity attacks as determined by the Florida Digital Service in consultation with the Florida Cybersecurity Advisory Council. The term includes, but is not limited to, public transportation as defined in s. 163.566(8); water and wastewater treatment facilities; public utilities and services subject to the jurisdiction, supervision, powers, and duties of the Public Service Commission; public buildings, including buildings operated by the state university system; hospitals and public health facilities; and financial services organizations.

(d) “Local government asset owner” means the local government owner or entity accountable and responsible for operation of critical infrastructure and its automation and control system. The term includes the operator of the automation and control system and the equipment under control.

(e) “Operational technology” means the hardware and software that cause or detect a change through the direct monitoring or control of physical devices, systems, processes, or events in critical infrastructure.

(4) Beginning July 1, 2022, a local government asset owner procuring automation and control system components, services, or solutions or entering into a contract for the construction, reconstruction, alteration, or design of a critical infrastructure facility must require that such components, services, and solutions conform to the ISA 62443 series of standards as referenced by the NIST CSF. Such local government asset owner shall ensure that all contracts for the construction, reconstruction, alteration, or design of a critical infrastructure facility require that installed automation and control system components meet the minimum standards for cybersecurity as defined in the ISA 62443 series of standards as referenced by the NIST CSF.

Section 2. The Florida Digital Service shall, in consultation with the Florida Cybersecurity Advisory Council, adopt rules to implement this act.

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