The Florida Senate

BILL ANALYSIS AND FISCAL IMPACT STATEMENT

(This document is based on the provisions contained in the legislation as of the latest date listed below.)

Prepared By: The Professional Staff of the Committee on Governmental Oversight and Accountability

BILL:	CS/SB 828
INTRODUCER:	Governmental Oversight and Accountability Committee and Senator Hutson
SUBJECT:	Critical Infrastructure
DATE:	February 2, 2022 REVISED:

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Ponder	McVaney	GO	**Fav/CS**
2.			MS	
3.			RC	

Please see Section IX. for Additional Information:

COMMITTEE SUBSTITUTE - Substantial Changes

I. Summary:

CS/SB 828 creates the Critical Infrastructure Standards and Procedures Act.

The bill sets forth legislative findings that:

- Standard definitions of the security capabilities for 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; and
- 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[1] is an appropriate resource for use in establishing such standard definitions.

The bill defines the terms:

- Automation and control system;
- Automation and control system component;
- Critical infrastructure;

[1] The ISA/IEC 62443 standards are one among many informational materials related to cybersecurity referenced by the *NIST Cybersecurity Framework*, which is a set of guidelines for mitigating organizational cybersecurity risks published by the United States National Institute of Standards and Technology.

- Local Government asset owner; and
- Operational technology.

The bill requires a "local government asset owner"[2] to:

- Require when 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 that such components, services, and solutions conform to the ISA 62443 series of standards as referenced by the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), beginning July 1, 2022.
- 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

The bill requires the Florida Digital Service, in consultation with the Florida Cybersecurity Advisory Council, to adopt rules to implement the act.

The bill takes effect on July 1, 2022.

II. Present Situation:

Cybersecurity and Critical Infrastructure

The United States depends on the reliable function of critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk.[3]

"Critical infrastructure" is defined in the U.S. Patriot Act of 2001 to mean "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[4] The critical infrastructure community includes public and private owners and operators, and other entities with a role in securing the Nation's infrastructure.

The Cybersecurity Enhancement Act of 2014 and the National Institute of Standards and Technology

The Cybersecurity Enhancement Act of 2014 grants the National Institute of Standards and Technology (NIST) power to guide the development of a "voluntary, industry-led set of

[2] The bill defines a "local government asset owner" to mean a local government owner or entity accountable and responsible for the 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.
[3] *Framework for Improving Critical Infrastructure Cybersecurity*, (NIST CSF), National Institute of Standards and Technology, April 16, 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
[4] 42 U.S.C. § 5195c(e).

standards . . . to cost-effectively reduce cyber risks to critical infrastructure."[5] NIST implements the Cybersecurity Act through its NIST Cybersecurity Framework (NIST CSF),[6] which provides a common organizing structure for multiple approaches to cybersecurity by assembling standards, guidelines and practices that are currently working effectively in the industry.[7]

The NIST CSF offers a flexible way to address cybersecurity, including cybersecurity's effect on physical, cyber, and people dimensions. It is applicable to organizations relying on technology, whether their cybersecurity focus is primarily on information technology, industrial control systems, cyber-physical systems, or connected devices more generally.

The NIST CSF provides a common system of classification for organizations to:
- Describe their current cybersecurity posture;
- Describe their target state for cybersecurity;
- Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
- Assess progress toward the target state; and
- Communicate among internal and external stakeholders about cybersecurity risk.

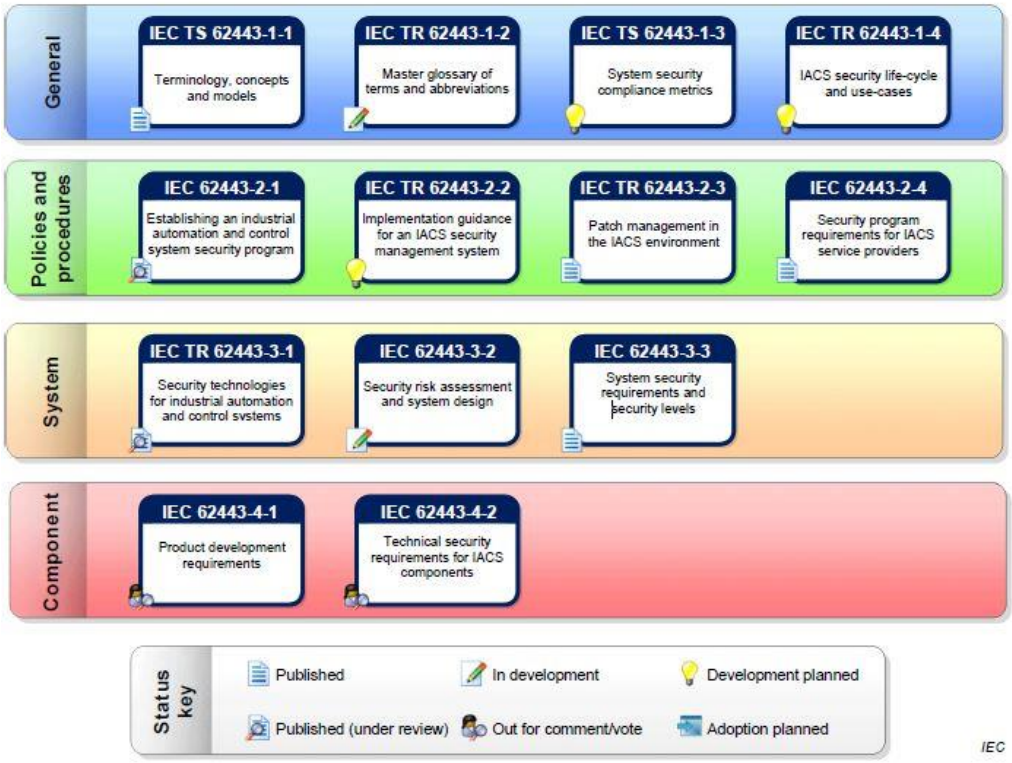
ISA 62443 Series of Standards

The NIST CSF references several informative standards relevant to cybersecurity, including the ISA/IEC 62443 (ISA 62443) which was jointly developed by the International Society of Automation (ISA)[8] and the International Electrotechnical Commission (IEC).[9] ISA 62443 addresses security issues unique to industrial automation and control systems (IACS) throughout their lifecycle. The ISA 62443 can be applied to any industrial environment, including critical infrastructure facilities, such as power utilities or nuclear plants, as well as in the health and transport sectors. Thus, the standards illustrate methods to manage distinctive challenges related to the IACS environments, including: (i) the relative criticality of data confidentiality in facilities operations or functions; (ii) potential dangers to personnel, the environment, and society in the event of cyber-physical failures; (iii) the relative difficulty of applying common information technology security techniques without severe systems modifications; and (iv) unique approaches to ensuring systems reliability and integrity in industrial environments.

[5] *See* 15 U.S.C. § 272(e)(1)(A)(i). The Cybersecurity Enhancement Act of 2014 (S.1353) became public law 113- 274 on December 18, 2014, and may be found at: https: //www.congress.gov/bill/113th-congress/senatebill/1353/text.
[6] Version 1.0 of the NIST Framework was released in 2014, in response to EO 13,636 "Improving Critical Infrastructure Cybersecurity," issued on February 12, 2013. It was subsequently replaced with version 1.1 in 2018.
[7] NIST CSF, *supra* note 5.
[8] The International Society of Automation (ISA) is a professional association founded in 1945 to create a better world through automation.
[9] The Electrotechnical Commission (IEC) is a global membership organization. IEC International Standards reflect the global consensus and distilled wisdom of many thousand technical experts who are delegated by their countries to participate in the IEC. The participating experts are organized into technical committees and subcommittees (TC/SC). Each TC defines its scope and area of activity. IEC 62443 was a project of the TC 65, Industrial-process measurement, control and automation

The ISA 62443 is a family of documents structured into a multi-tier grouping of four parts: General (ISA 62443-1); Policies and procedures (ISA 62443-2); System (ISA 62443-3); and Component (ISA 62443-4).[10]

Figure 1: ISA 62443 Standards Overview[11]



ISA 62443-1 defines the elements necessary to establish a cybersecurity management system for industrial automation and control systems (IACS) and provides guidance on how to develop those elements. It defines IACS as a "collection of processes, personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process." ISA 62443-1 also lists the seven foundational requirements:

- Identification and authentication control;
- Use control;
- System integrity;
- Data confidentiality;
- Restricted data flow;
- Timely response to events; and

[10] Ron Brash, *The Ultimate Guide to Protecting OT Systems with IEC 62443* (June 23, 2021), https://verveindustrial.com/resources/blog/the-ultimate-guide-to-protecting-ot-systems-with-iec-62443/.

[11] Figure 1 illustrates the relationship of the different parts of the IEC 62443. *See* International Electrotechnical Commission, *Security for Industrial Automation and Control Systems – Part 4-1: Secure product development lifecycle requirements* https://webstore.iec.ch/preview/info_iec62443-4-1%7Bed1.0%7Db.pdf.

- Resource availability.

ISA 62443-2, policy and procedures, defines the elements necessary to establish a cybersecurity management system for IACS and provides guidance on how to develop those elements. Specifies a comprehensive set of requirements covering IACS service providers that can be used during integration and maintenance activities. ISA 62443-2-4, provides the basis for a larger ISA 62443 initiative to develop "profiles" that address the nuances and realities in different industrial environments, for example, the unique requirements of oil and gas producers versus those of electricity generation and distribution.

ISA 62443-3 sets forth the requirements at the system level, including:
- Defining a system under consideration for an IACS;
- Partitioning the system under consideration into zones and conduits;
- Assessing risk for each zone and conduit;
- Establishing the target security level for each zone and conduit; and
- Documenting the security requirements.

ISA 62443-3-3 provides detailed technical control system requirements associated with the seven foundational requirements provided in ISA 62442-1 including defining the requirements for control system capability security levels. Such requirements would be used by various members of the IACS community.

ISA 62443-4 defines a secure development life-cycle for purpose of developing and maintaining secure products. This life-cycle description includes security requirements definition, secure design, secure implementation (including coding guidelines), verification and validation, defect management, patch management and product end-of-life. These requirements can be applied to new or existing processes for developing, maintaining and retiring hardware, software or firmware.

The ISA 62443, like most standards and frameworks, offers guidance to improve existing processes for technology project scoping, vendor selection and procurement. For example, an organization that wants to create a machine cell for a new process with a minimum level of security to prevent accidental issues can reference the requirements in ISA-62443-3-3 and other sibling documents to develop pre-selection criteria and achieve its objective. The standards can also be used to dictate how factory and site acceptance testing includes security verification before handoff.[12]

Cybersecurity Intrusions

Oldsmar Water System

On February 5, 2021, hackers remotely accessed the water treatment plant of the city of Oldsmar and changed the levels of lye in the drinking water. At a press conference on February 8, 2021, Sheriff Bob Gualtieri of Pinellas County stated that the hacker changed the level of sodium

[12] Brash, *supra* note 11.

hydroxide– also known as lye[13] (the main ingredient in liquid drain cleaners) – from about 100 parts per million to 11,100 parts per million, dangerous levels that could have badly sickened residents if it had reached their homes.[14] The intrusion lasted three to five minutes and was mitigated before it could reach the drinking supply and inflict harm.

Colonial Pipeline

On May 7, 2021, Colonial Pipeline, which carries refined gasoline and jet fuel from Texas up the East Coast to New York, shut down its system in response to a ransomware cyberattack.[15] The company quickly notified the Federal Bureau of Investigation (FBI) on the day of the attack. The FBI attributed the cyberattack to DarkSide, a group believed to be based in Russia or Eastern Europe. The pipeline was shut down for approximately six days.

In June 2021, the chief executive of the pipeline company told a Senate committee that it is believed that the cybercriminals accessed its computer via an old virtual private network - commonly known as a V.P.N. - that the company no longer used.[16] It is believed that the damage to the pipeline could have been worse had the company not paid the ransom to DarkSide. Investigators were able to trace 75 Bitcoins worth more than $4 million through cryptocurrency accounts and recover much of the ransom paid by the company.[17]

Bowman Avenue Dam – Rye Brook N.Y.

The Bowman Avenue Dam is located in Rye Brook, New York, a village of about 9,500 residents. The dam's floodgate is only about 15 feet long and two and half feet high. It was primarily built to keep the Blind Brook, a small babbling creek, from flooding homes and businesses nearby. Despite its unassuming size, the dam was a target of a cyberattack in 2013. Seven Iranian computer hackers chose to penetrate the dam's computer-guided controls as part of a plot that also breached or shut down over forty of the nation's largest financial institutions.[18] The attempt failed because the dam was under repair and offline at the time. However, the incident worried American investigators because the attack was aimed at seizing control of a piece of infrastructure.

The National Institute of Standards and Technology in Florida Statutes

Section 531.39, F.S., provides that weights and measures that are traceable to the United States prototype standards supplied by the Federal Government, or approved as being satisfactory by the National Institute of Standards and Technology (NIST), shall be the state primary standards of weights and measures, and shall be maintained in such calibration as prescribed by

[13] Lye is the main ingredient in liquid drain cleaners and also used to control water acidity and remove metals from drinking water in water treatment plants.
[14] Treatment Plant Intrusion Press Conference, February 8, 2021, https://www.youtube.com/watch?v=MkXDSOgLQ6M (last visited December 7, 2021).
[15] David E. Sanger, Clifford Krauss and Nicole Perlroth, *Cyberattack Forces a Shutdown of a Top U.S. Pipeline*, New York Times, May 8, 2021, https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html.
[16] Clifford Krauss, *Colonial Pipeline chief says an oversight let hackers into its system,* New York Times, June 8, 2021, https://www.nytimes.com/2021/06/08/business/colonial-pipeline-hack.html?searchResultPosition=4.
[17] Katie Benner, Nicole Perloth, *U.S. Seizes Share of Ransom From Hackers in Colonial Pipeline Attack.*
[18] Joseph Berger, *A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case*, New York Times, March 25, 2016, https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html.

the National Institute of Standards and Technology. The Department of Agriculture and Consumer Services is required to regulations regarding technical requirements for commercial weighing and measuring devices, which conform to those adopted by the NIST to the extent possible.[19]

The Department of Management Services (DMS), acting through the Florida Digital Service, is the lead entity responsible for establishing standards and processes for assessing state agency cybersecurity risks and determining appropriate security measures.[20] These standards and processes are required to be consistent with generally accepted technology best practices, including the NIST CSF.[21] Additionally, the DMS, acting through the Florida Digital Service, must establish procedures for procuring information technology commodities and services that require the commodity or service to meet the NIST CSF.[22]

III. Effect of Proposed Changes:

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

This section provides legislative findings 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; and
- 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.

This section defines the following terms:

- Automation and control system;
- Automation and control system component;
- Critical infrastructure;
- Local government asset owner; and
- Operation technology.

"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.

"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. Control systems include, but are not limited to:

[19] Section 531.40, F.S.
[20] Section 282.318(3), F.S.
[21] *Id*.
[22] Section 282.318(3)(c)13, F.S.

- 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;
- 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; and
- 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.

"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 Florida Public Service Commission;
- Public buildings, including those operated by the State University System;
- Hospitals and public health facilities; and
- Financial services organizations.

"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.

"Operation 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.

This section requires a local government asset owner, beginning on July 1, 2022, when 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 to 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 components meet the minimum standards for cybersecurity as defined in the ISA 62443 series of standards as referenced by the NIST CSF.

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

Section 3 provides that the bill takes effect July 1, 2022.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

Article VII, s. 18(a) of the State Constitution provides, in relevant part, that: "No county or municipality shall be bound by any general law requiring such county or municipality to spend funds ... unless the legislature has determined that such law fulfills an important state interest and unless: the law requiring such expenditure is approved by two-thirds vote of the membership of each house of the legislature;

If counties and municipalities complying with the bill's requirements related to the ISA 62443 series of standards as referenced by the NIST CSF is deemed to be "requiring" an expenditure under the mandates provision, the legislature may want to consider adding a legislative finding that the bill fulfills an important state interest to ensure such requirements are binding upon counties and municipalities.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

D. State Tax or Fee Increases:

None.

E. Other Constitutional Issues:

None identified.

V. None identified. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

The entities that charge a fee for access to the ISA 62443 series of standards as referenced by the NIST CSF will experience a positive fiscal impact.

C. Government Sector Impact:

Local governmental entities who qualify as a "local government asset owner" will incur additional costs in meeting the requirements under the bill for specified compliance with the ISA 62443 series of standards as referenced by the NIST CSF.

VI. Technical Deficiencies:

None.

VII. Related Issues:

None.

VIII. Statutes Affected:

This bill creates section 282.32, F.S.

IX. Additional Information:

A. Committee Substitute – Statement of Substantial Changes:
(Summarizing differences between the Committee Substitute and the prior version of the bill.)

CS by Governmental Oversight and Accountability on February 2, 2022:
The amendment:

- Requires "local government asset owners" - a local government owner or entity accountable and responsible for the operation of critical infrastructure and its automation and control system - to:
  - Require when 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 that such components, services, and solutions conform to the ISA 62443 series of standards as referenced by the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), beginning July 1, 2022.
  - 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.
- Grants rulemaking authority to the Florida Digital Service, in consultation with the Florida Cybersecurity Advisory Council.
- Removes the grant of civil liability.

B. Amendments:

None.