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:	SB 828
INTRODUCER:	Senator Hutson
SUBJECT:	Critical Infrastructure
DATE:	February 1, 2022
REVISED:	

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Ponder	McVaney	GO	**Pre-meeting**
2.			MS	
3.			RC	

I. Summary:

SB 828 creates the Critical Infrastructure Standards and Procedures Act.

The bill sets forth a legislative finding 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. As part of the legislative finding, the bill notes the importance of cybersecurity standards and instructs that the internationally recognized ISA/IEC 62443 standards (IEC 62443)[1] define a set of measures and benchmarks that 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.

The bill requires an asset owner,[2] beginning July 1, 2024, to 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 within IEC 62443, including annual risk assessments and creation of a mitigation plan.

The bill requires specified procurements to conform to the IEC 62443 beginning July 1, 2026. Specifically, 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 must require that such items conform to the IEC 62443. Additionally, contracts

[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.

[2] The bill defines the term "asset owner" to mean 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.

awarded for specified activities[3] must require that installed automation and control components meet the minimum standards for cybersecurity as defined by the IEC 62443.

The bill provides for specified procedures, determinations, a condition of immunity, and remedies for any civil action based on a cybersecurity-breach related claim, including a civil action brought by the Department of Law Enforcement (department) under the bill.

The bill authorizes the department to institute an appropriate legal proceeding, including a civil action, against a party if it has reason to believe that the party - a business, service provider, or other person or entity - is in violation of the compliance requirements set forth in the bill and that proceedings would be in the public interest. The bill gives the department discretion to grant a party a 30-day cure period and issue a letter of guidance under a specified procedure. The department is permitted to bring a legal proceeding against the business for the alleged violation.

The bill grants the department rule-making authority in consultation with the Florida Digital Service and the Florida Cybersecurity Advisory Council.

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.[4]

"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."[5] 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 standards . . . to cost-effectively reduce cyber risks to critical infrastructure."[6] NIST implements

[3] Contracts awarded for construction, reconstruction, alteration, design, or commissioning of facilities identified as critical infrastructure.
[4] *Framework for Improving Critical Infrastructure Cybersecurity*, (NIST Framework), National Institute of Standards and Technology, April 16, 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
[5] 42 U.S.C. § 5195c(e).
[6] *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.

the Cybersecurity Act through its NIST Framework,[7] 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.[8]

The NIST Framework 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 Framework 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/IEC 62443 Series of Standards

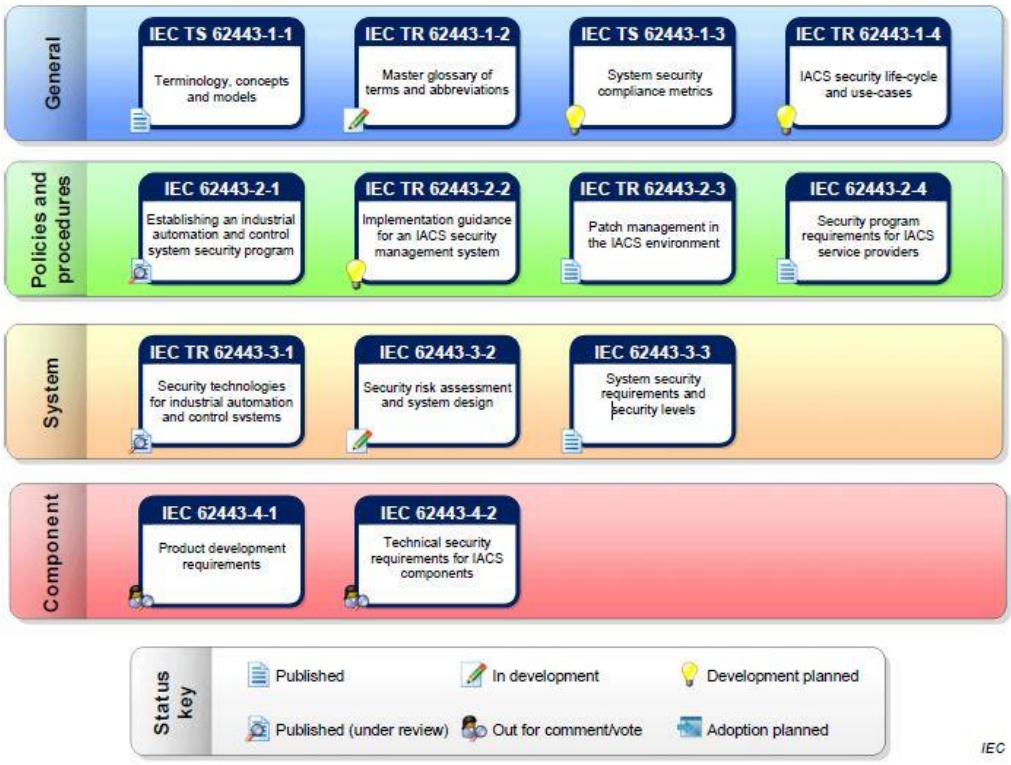
The NIST Framework references several informative standards relevant to cybersecurity, including the ISA/IEC 62443 (IEC 62443) which was jointly developed by the International Society of Automation (ISA)[9] and the International Electrotechnical Commission (IEC).[10] IEC 62443 addresses security issues unique to industrial automation and control systems (IACS) throughout their lifecycle. IEC 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.

The IEC 62443 is a family of documents structured into a multi-tier grouping of four parts: General (IEC 62443-1); Policies and procedures (IEC 62443-2); System (IEC 62443-3); and Component (IEC 62443-4).[11]

---

[7] 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.
[8] NIST Framework, *supra* note 4.
[9] The International Society of Automation (ISA) is a professional association founded in 1945 to create a better world through automation.
[10] 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
[11] 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/.

Figure 1: IEC 62443 Standards Overview[12]



IEC 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." IEC 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
- Resource availability.

IEC 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. IEC 62443-2-4, provides the basis for a larger

[12] 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.

IEC 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.

IEC 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.

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

IEC 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 IEC 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 IEC-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.[13]

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 hydroxide– also known as lye[14] (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.[15] The intrusion lasted three to five minutes and was mitigated before it could reach the drinking supply and inflict harm.

[13] Brash, *supra* note 11.
[14] 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.
[15] Treatment Plant Intrusion Press Conference, February 8, 2021, https://www.youtube.com/watch?v=MkXDSOgLQ6M (last visited December 7, 2021).

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.[16] 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.[17] 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.[18]

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.[19] 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.

Florida Department of Law Enforcement

Section 20.201, F.S., creates the Department of Law Enforcement (FDLE). FDLE is a criminal justice agency with statewide jurisdiction. FDLE's mission is to promote public safety and strengthen domestic security by providing services in partnership with local, state, and federal criminal justice agencies to prevent, investigate, and solve crimes while protecting Florida's citizens and visitors. Through its seven Regional Operations Centers and five Divisions,[20] FDLE delivers investigative, forensic, training and protection/security services to Florida's criminal justice community.

[16] 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.
[17] 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.
[18] Katie Benner, Nicole Perloth, *U.S. Seizes Share of Ransom From Hackers in Colonial Pipeline Attack*.
[19] 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.
[20] Executive Direction and Business Support, Criminal Investigations and Forensic Science, Criminal Justice Information, Criminal Justice Professionalism and Florida Capitol Police.

Civil Immunity

Florida law provides civil immunity to certain individuals in specified circumstances who, acting in good faith, attempt to render aid to others.[21] Section 937.021, F.S., currently provides civil immunity for specified entities requested by law enforcement to record, report, transmit, display, or release information pertaining to a missing person if such entity complied with the request in good faith.[22] These entities include:

- The FDLE, a state or local law enforcement agency, and agency personnel;
- A radio or television network, broadcaster, or other media representative; or
- A dealer of communications services as defined in s. 202.11, F.S.[23]

Entities who report, transmit, display, or release information pertaining to a missing person are presumed to have acted in good faith.[24] The presumption of good faith is not overcome if a technical or clerical error is made by an agency, employee, individual, or entity acting at the request of the local law enforcement agency having jurisdiction or if the missing person information is incomplete or incorrect because the information received from the local law enforcement agency was incomplete or incorrect.[25]

Negligence

As developed by the common law, a cause of action for negligence arises where one's "failure to use that degree of care which a reasonably careful person would use under like circumstances" causes injury.[26] Common law negligence is open-ended and divorced from intent,[27]"allow[ing] the plaintiff to claim that any given conduct was negligent."[28]

While negligence has its roots in common law, legislative enactments play an important role in shaping standards of conduct.[29] Proof that a defendant violated a statute——can be categorized in a negligence case in one of three ways, depending on the statute's purpose: (1) violation of a strict liability statute designed to protect a particular class of persons who are unable to protect themselves, constituting negligence per se; (2) violation of a statute establishing a duty to take precautions to protect a particular class of persons from a particular type of injury, also constituting negligence per se; (3) violation of any other kind of statute, constituting mere prima facie evidence of negligence.

---

[21] For example, Section 768.13, F.S. (also known as Florida's Good Samaritan Act (GSA)) provides immunity from civil liability for persons acting in good faith who render emergency care and treatment to individuals in need of assistance. Under the GSA, immunity from civil liability is available to any person who gratuitously and in good faith renders emergency assistance without the objection of a victim, if the person acts as a reasonably prudent person would act under similar circumstances.

[22] Section 937.021(5)(a), F.S.

[23] Examples of a dealer of communications services include a cable or satellite television service provider, a telephone service provider, or a mobile communication service provider. s. 937.021, F.S.

[24] Section 937.021(5)(c), F.S.

[25] *Id.*

[26] *London v. Atl. Mut. Ins. Co.*, 689 So.2d 424, 425 (Fla. 4th DCA 1997).

[27] *Booth v. Mary Carter Paint Co.*, 182 So.2d 292, 299 (Fla. 2d DCA 1966).

[28] Dan B. Dobbs, *The Law of Torts* § 110, at 257 (2000).

[29] *Kohl v. Kohl*, 149 So. 3d 127, 131–32 (Fla. 4th DCA 2014) (citing W. Page Keeton et al., *Handbook on the Law of Torts* § 35 (3d ed. 1964)).

For there to be an "actionable negligence claim against a government entity, there must be a common law or statutory duty regarding the alleged negligent conduct."[30]

Sovereign Immunity

Sovereign immunity protects the sovereign from being sued without its consent.[31] . At common law, the state possessed immunity from suit as an aspect of its sovereignty. The doctrine of sovereign immunity flows from the concept that one could not sue the king in his own courts; hence the phrase 'the king can do no wrong.'"[32] The doctrine has been adopted and codified by the Florida Legislature.[33]

Article X, section 13 of the State Constitution, however, allows the Legislature to abrogate the state's sovereign immunity.[34] The Legislature, in accordance with this provision, effectuated a limited waiver of sovereign immunity in s. 768.28, F.S. The sovereign immunity statute authorizes suits in tort against the State and its agencies and political subdivisions for damages resulting from the negligence of government employees acting in the scope of their employment.[35] The waiver applies only to "injury or loss of property, personal injury, or death caused by the negligent or wrongful act or omission of any employee of the agency or subdivision while acting within the scope of the employee's office or employment ...." [36]

Section 768.28(5), F.S., provides that the state, its agencies, or subdivisions shall not be liable to pay any claim or judgment by any one person which exceeds the sum of $200,000.[37] If there are multiple claims or judgments arising out of the same incident or occurrence, the total amount the state, its agencies, or subdivisions may be liable for is $300,000.[38].

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 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, that conform to those adopted by the NIST to the extent possible.[39]

---

[30] *Moore v. Dep't of Corr.*, 833 So. 2d 822, 824 (Fla. 4th DCA 2002) (citing *Hinckley v. Palm Beach County Bd. of Comm'rs*, 801 So. 2d 193, 194-95 (Fla. 4th DCA 2001)).
[31] *Town of Gulf Stream v. Palm Beach Cty.*, 206 So. 3d 721, 725 (Fla. 4th DCA 2016); *City of Fort Lauderdale v. Israel*, 178 So.3d 444, 446 (Fla. 4th DCA 2015)
[32] *Cauley v. City of Jacksonville*, 403 So.2d 379, 381 (Fla. 1981).
[33] *See generally* s. 2.01, F.S.
[34] Article X, Section 13, Fla. Const.
[35] Section 768.28, F.S.
[36] Section 768.28(1), F.S.
[37] Section 768.28(5), F.S.
[38] *Id.*
[39] Section 531.40, F.S.

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.[40] These standards and processes are required to be consistent with generally accepted technology best practices, including the NIST Cybersecurity Framework for cybersecurity.[41] 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 Cybersecurity Framework.[42]

III. Effect of Proposed Changes:

The bill includes a series of whereas clauses that provide background information on the importance of maintaining the security of operational technologies that operate critical infrastructure and how such critical infrastructure is at risk of experiencing cybersecurity intrusion.

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

Section 2 creates s. 943.6873, F.S., to set forth the legislative finding 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. This section explains that 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 (IEC 62443). 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.

This section defines the following terms:
- Asset owner;
- Automation and control system;
- Automation and control system component;
- Critical infrastructure;
- Cybersecurity-breach-related claim;
- Department; and
- Operation technology.

"Asset owner" is defined to mean the public or private owner of, or the entity accountable and responsible for operation of, the critical infrastructure and the automation and control system.

[40] Section 282.318(3), F.S.
[41] *Id*.
[42] Section 282.318(3)(c)13, F.S.

The asset owner is also the operator of the automation and control system components and the equipment under its control.

"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.

"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:

- 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;
- 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
- Associated internal, human, network used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes as defined by the International Society of Automation IEC 62443.

"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.

"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.

"Department" means the Department of Law Enforcement.

"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.

Section 2 requires the asset owner, beginning on July 1, 2024, to 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 IEC 62443, including annual risk assessments and creation of a mitigation plan. (July 2024 General Requirements)

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 must require that such items conform to the IEC 62443. (July 2026 Procurement Requirements) 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 IEC 62443.

Section 2 also provides that in any civil action based on a cybersecurity-breach related claim, including a civil action brought by the Department of Law Enforcement (department)[43] under the bill:

- A court shall determine as a matter of law whether the defendant made a good faith effort to comply with July 2024 General Requirements or the July 2026 Procurement Requirements, as applicable.
- The defendant is immune from civil liability upon determination by the court of a good faith effort by defendant.
- The plaintiff may proceed with the action if the court determines that the defendant did not make such a good faith effort.
- 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:
  - Issue a temporary or permanent injunction.
  - Impose a civil penalty of not more than $2,500 for each unintentional violation or $7,500 for each intentional violation.
  - Award reasonable costs of enforcement, including reasonable attorney fees and costs.
  - Grant any other relief as the court deems appropriate.

Section 2 authorizes the department to institute an appropriate legal proceeding, including a civil action, against a party if it has reason to believe that that party - a business, service provider, or other person or entity - is in violation of the compliance requirements set forth in the bill and that proceedings would be in the public interest. Upon providing written notice, the department may allow a party a 30-day period to cure the alleged violation. Under the bill, 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.

This section allows the department discretion to issue a letter of guidance if the party[44] cures the alleged violation. Specifically, if the alleged violation is cured to the department's satisfaction and the party provides proof of such cure, the department may issue a letter of guidance to the party providing notice that a 30-day cure period for any future violation will not be offered.

[43] The Department of Law Enforcement is a criminal justice agency and is currently not charged with bringing forth civil suits in any capacity.
[44] The business, service provider, or other person or entity.

Should the party fail to cure the violation within 30 days, the department may bring a legal proceeding against the business for the alleged violation.

This section grants the department with rule making authority in consultation with the Florida Digital Service and the Florida Cybersecurity Advisory Council.

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; [or] . . . the expenditure is required to comply with a law that applies to all persons similarly situated, including the state and local governments. . .."

If counties and municipalities complying with the bill's requirements related to the IEC 62443 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. As drafted, the bill seems to apply to all persons similarly situated (governmental entities responsible for operation of critical infrastructure) including state agencies, universities, 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:

Article I, section 21, of the State Constitution, part of the constitutional "Declaration of Rights" states that ":[t]he courts shall be open to every person for redress of any injury, and justice shall be administered without sale, denial or delay."

The scope of the access-to-courts provision has been addressed by Florida courts on multiple occasions.[45] In *Kluger,* the Florida Supreme Court interpreted the access-to-courts guarantee to mean that the legislature cannot abolish a statutory or common law right that existed prior to the adoption of the Declaration of Rights without providing a reasonable alternative, unless the legislature can show an overpowering public necessity for the abolishment of such right, and no alternative method of meeting such public necessity can be shown.[46] Though *Kluger* spoke in terms of total abolishment of a right, the scope of the protection extends to circumstances in which legislative action significantly obstructs the right to access to the courts.[47] Thus, a statute restricting access to the courts is not permitted unless one of the *Kluger* exceptions is met: (i) the legislature provides a reasonable alternative remedy or commensurate benefit; or (ii) the legislature makes a showing of overpowering public necessity for the abolishment of the right and no alternative method of meeting such public necessity."[48]

Here, the bill provides that if a court determines that a defendant in any civil action based on a cybersecurity-breach-related claim made a good faith[49] effort to comply with the July 2024 General Requirements or the July 2026 Procurement Requirements, the defendant is immune from liability. The exemption from liability based on a "good faith effort to comply" could be interpreted as an obstacle to an injured party's right to access the courts in a claim of negligence related to a cybersecurity-breach related event.

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

Private entities who qualify as an "asset owner" will incur additional costs in meeting the requirements under the bill for specified compliance with the IEC 62443.

C. Government Sector Impact:

Governmental entities who qualify as an "asset owner" will incur additional costs in meeting the requirements under the bill for specified compliance with the IEC 62443.

---

[45] *See, e.g., Nationwide Mut. Fire Ins. Co. v. Pinnacle Med., Inc.,* 753 So.2d 55 (Fla.2000); *Psychiatric Assocs. v. Siegel,* 610 So.2d 419 (Fla.1992); *Smith v. Dep't of Ins.,* 507 So.2d 1080 (Fla.1987); *Carter v. Sparkman,* 335 So.2d 802 (Fla.1976), *receded from on other grounds in Aldana v. Holub,* 381 So.2d 231 (Fla.1980); *Kluger v. White,* 281 So.2d 1 (Fla.1973); *Lloyd v. Farkash,* 476 So.2d 305 (Fla. 1st DCA 1985).

[46] *Kluger v. White*, 281 So. 2d 1, 4 (Fla. 1973).

[47] *Weaver v. Myers*, 229 So. 3d 1118, 1140 (Fla. 2017); *Mitchell v. Moore*, 786 So. 2d 521, 527 (Fla. 2001)("…in order to find that a right has been violated it is not necessary for the statute to produce a procedural hurdle which is absolutely impossible to surmount, only one which is significantly difficult").

[48] *Samples v. Florida Birth-Related Neurological Injury Comp. Ass'n*, 114 So. 3d 912, 920 (Fla. 2013).

[49] Black's Law defines the term "good faith" to mean "a state of mind consisting in (1) honesty in belief or purpose, (2) faithfulness to one's duty or obligation, (3) observance of reasonable commercial standards of fair dealing in a given trade or business, or (4) absence of intent to defraud or to seek unconscionable advantage." Black's Law Dictionary (11th ed. 2019).

Additionally, the Department of Law Enforcement will incur indeterminate costs in meeting its responsibilities under the bill.

VI. Technical Deficiencies:

None.

VII. Related Issues:

None.

VIII. Statutes Affected:

This bill creates section 943.6873, F.S.

IX. Additional Information:

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

None.

B. Amendments:

None.