


# Energy, Communications & Cybersecurity Subcommittee

**Tuesday, March 21, 2023**
**2:00 pm - 6:00 pm**
**Reed Hall (102 HOB)**

**Meeting Packet**

**Paul Renner**
**Speaker**

**Mike Giallombardo**
**Chair**

# The Florida House of Representatives

**Commerce Committee**

**Energy, Communications & Cybersecurity Subcommittee**

**Paul Renner**
**Speaker**

**Mike Giallombardo**
**Chair**

## Meeting Agenda

Tuesday, March 21, 2023
2:00 pm – 6:00 pm
Reed Hall (102 HOB)

I. Call to Order

II. Roll Call

III. Welcome and Opening Remarks

**IV. Consideration of the following bill(s):**

- HB 821 Renewable Energy Cost Recovery by Yeager
- HB 1221 Broadband Internet Service Providers by Tomkow
- HB 1437 Pub. Rec./Broadband Opportunity Program Information/DEO by Esposito
- HB 1511 Cybersecurity by Giallombardo

**Consideration of the following proposed committee substitute(s):**

- PCS for HB 1025 -- Government Vehicles
- PCS for HB 1331 -- Municipal Utilities

V. Closing Remarks

VI. Adjournment

HB 821

**HOUSE OF REPRESENTATIVES STAFF ANALYSIS**

**BILL #:** HB 821 Renewable Energy Cost Recovery
**SPONSOR(S):** Yeager
**TIED BILLS:** **IDEN./SIM. BILLS:** SB 1162

| REFERENCE | ACTION | ANALYST | STAFF DIRECTOR or BUDGET/POLICY CHIEF |
|---|---|---|---|
| 1) Energy, Communications & Cybersecurity Subcommittee | | Walsh | Keating |
| 2) State Administration & Technology Appropriations Subcommittee | | | |
| 3) Commerce Committee | | | |

## SUMMARY ANALYSIS

The Public Service Commission (PSC) has broad jurisdiction over the rates and service of public (investor-owned) electric and natural gas utilities in Florida. The PSC sets rates for these utilities through various mechanisms to allow the utilities to recover their legitimate costs of providing service, including a return on the utility's prudent capital investments.

Currently, the fuel required by public utilities to provide service in Florida is purchased from competitive providers in an open market. These purchases, if deemed prudent by the PSC, are passed through to utility customers with no markup for profit to the utility. With one exception for a pilot project, public utility investments in fuel production projects are not included in the rates of electric or natural gas public utilities.

Renewable natural gas (RNG) is the gaseous product of the decomposition of organic matter, processed into a pipeline-quality gas that is fully interchangeable with conventional natural gas. Primary sources of RNG include landfills, livestock operations, and wastewater treatment facilities. Hydrogen fuel is produced predominantly from natural gas but can also be produced, at a greater cost, by electrolysis powered by renewable energy.

The bill allows electric and natural gas public utilities to recover through rates:

- The costs of contracts for the purchase of RNG and hydrogen, with pricing above the current market value of natural gas, if the PSC finds that the contract promotes the development or use of renewable energy resources in the state and provides fuel diversification.
- Prudently-incurred costs for RNG and hydrogen fuel infrastructure projects, including but not limited to:
    - Capital investment in projects necessary to prepare or produce RNG and hydrogen fuel for pipeline distribution and usage;
    - Capital investment in facilities, including pipelines, necessary to inject and deliver RNG and hydrogen fuel throughout this state;
    - RNG and hydrogen fuel storage facilities;
    - Operation and maintenance expenses associated with any such RNG and hydrogen fuel infrastructure projects; and
    - An appropriate return on investment consistent with the return allowed for other utility plants used to provide service to customers.

The bill provides for cost recovery of prudent infrastructure project costs through an appropriate mechanism administered by the PSC.

The bill does not appear to impact state or local government revenues or expenses.

The bill provides an effective date of July 1, 2023.

## FULL ANALYSIS

## I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

**Current Situation**

Rate Setting for Public Utilities

The Public Service Commission (PSC) has broad jurisdiction over the rates and service of public (investor-owned) electric and natural gas utilities in Florida.[1] Under this broad grant of authority, and through more specific grants of authority in Chapter 366, F.S., the PSC sets rates for such utilities through various mechanisms, each of which is established in a separate administrative proceeding:

- Base rates (set for electric and natural gas utilities)
  - Adjusted as needed in a general rate case, conducted through a formal evidentiary hearing for electric utilities and either a formal or informal proceeding for natural gas utilities.[2]
  - Designed to recover most operations and maintenance expenses, depreciation expense (recovery of capital investment over time), and a return on capital investment.
- Fuel and purchased power cost recovery charges (set for electric utilities only)
  - Adjusted annually through a formal evidentiary hearing.
  - Designed to recover the costs of fuel and the energy component of wholesale power purchases.
  - By PSC order, may include recovery of certain capital investments, including a return on investment.
- Purchased gas adjustment charges (set for natural gas utilities only)
  - Adjusted annually through a formal evidentiary hearing.
  - Designed to recover the costs of wholesale natural gas purchases.
- Capacity cost recovery charges (set for electric utilities only)
  - Adjusted annually through a formal evidentiary hearing.
  - Designed to recover costs of the capacity component of wholesale power purchases.
  - By statute, may include recovery of certain costs related to development of new nuclear power plants, including a return.[3]
- Environmental cost recovery charges (set for electric utilities only)
  - Adjusted annually through a formal evidentiary hearing.
  - Designed to recover costs to comply with government-mandated environmental standards.
  - By statute, may include recovery of certain capital investments, including a return on investment.[4]
- Storm protection plan cost recovery charges (set for electric utilities only)
  - Adjusted annually through a formal evidentiary hearing.
  - Designed to recover costs to implement PSC-approved storm protection plans.
  - By statute, may include recovery of certain capital investments, including a return on investment.[5]
- Energy conservation and efficiency cost recovery charges (set for electric and natural gas utilities)
  - Adjusted annually through a formal evidentiary hearing.
  - Designed to recover costs of implementing PSC-approved energy conservation and efficiency programs.

[1] *See, e.g.,* ss. 366.01, 366.04(1), 366.041, 366.05(1), and 366.06, F.S.
[2] A natural gas utility or a public electric utility whose annual sales to end-use customers amount to less than 1,000 gigawatt hours may request that the PSC process the utility's petition for rate relief using an informal "proposed agency action" procedure. S. 366.06(4), F.S.
[3] S. 366.93, F.S.
[4] S. 366.8255, F.S.
[5] S. 366.96, F.S.

As required by law, the PSC sets base rates to allow utilities to recover their legitimate costs of providing service (not otherwise recovered through another cost recovery mechanism), including a return on the utility's prudent capital investments ("rate base").[6] In each rate case, the PSC sets a "reasonable" rate of return on equity for each utility to apply to its rate base. This rate is typically applied to the utility's investments that the PSC allows to be recovered through cost recovery mechanisms other than base rates.

Currently, the fuel required by public utilities to provide service in Florida is purchased from competitive providers in an open market. As noted above, public utilities recover their fuel costs through one of two mechanisms; electric public utilities recover their fuel costs through fuel and purchased power cost recovery charges, and natural gas public utilities recover their wholesale natural gas costs through purchased gas adjustment charges. The PSC determines the prudence of a utility's fuel costs largely by determining whether the utility contracted for fuel on reasonable terms based on what was known or should have been known by purchasers in the market at that time. These costs are passed through to utility customers with no markup for profit to the utility.

With one exception, public utility investments in fuel production projects are not included in the rates of electric or natural gas public utilities. In 2021, the PSC approved a comprehensive Stipulation and Settlement Agreement to resolve a pending proceeding to set base rates for Florida Power & Light Company (FPL). Among other things, the settlement authorized FPL to implement a "Green Hydrogen"[7] pilot project to evaluate how its combustion turbine units operate with a hydrogen fuel mix and learn how a hydrogen fuel production facility can be effectively used on-site with combustion turbine units. The project uses energy from a solar-powered facility to convert water into green hydrogen through electrolysis, which will then be burned as fuel in a nearby FPL natural-gas powered generator. The settlement allowed FPL to include in its base rates estimated costs of $65 million for the project.[8]

Renewable Energy

Florida law provides that it is in the public interest to promote the development of renewable energy resources to help diversify fuel types for electric production, minimize the volatility of fuel costs, encourage investment within the state, improve environmental conditions, and make Florida a leader in new and innovative technologies.[9] The law defines renewable energy as energy produced from a method that uses one or more of the following fuels or energy sources: hydrogen produced or resulting from sources other than fossil fuels, biomass, solar energy, geothermal energy, wind energy, ocean energy, and hydroelectric power.[10]

*Hydrogen*

Hydrogen can be produced using a process called electrolysis, which splits water into hydrogen and oxygen.[11] When renewable energy is used as the source of electricity to power an electrolyzer,[12] the resulting hydrogen can result in zero greenhouse gas emissions[13] and is referred to as green hydrogen. Electrolyzers range in size, varying from small appliance-sized units to larger-scale central production facilities that can be tied directly to renewable forms of electricity production to power the unit.[14]

[6] Ss. 366.041(1) and 366.06(1), F.S.
[7] See *Hydrogen*, below.
[8] *Order No. PSC -2021-0446-S-EI*, issued December 2, 2021, in PSC Docket No. 20210015.
[9] S. 366.91, F.S.
[10] S. 366.91(2)(e), F.S. The term also includes waste heat from sulfuric acid manufacturing operations and electrical energy pro duced using pipeline-quality synthetic gas produced from waste petroleum coke with carbon capture and sequestration.
[11] *Id*.
[12] The process of electrolysis uses an electrolyzer, which is a system that uses electricity to break water into hydrogen and oxygen. Cummins, Inc., *Electrolyzers 101: What They Are, How They Work, and Where They fit in a Green Economy*, https://www.cummins.com/news/2020/11/16/electrolyzers-101-what-they-are-how-they-work-and-where-they-fit-green-economy (last visited Mar. 18, 2023).
[13] Office of Energy Efficiency & Renewable Energy, *Hydrogen Production: Electrolysis*, U.S. Department of Energy, https://www.energy.gov/eere/fuelcells/hydrogen-production-electrolysis (last visited Mar. 18, 2023).
[14] *Id*.

Some alternative methods of producing hydrogen, mainly grey hydrogen[15] and blue hydrogen,[16] use methane or coal to power the production process.[17] Another alternative method of producing hydrogen, turquoise hydrogen, uses methane through the process of pyrolysis, which creates a reaction to generate hydrogen and solid carbon, which means that there are no carbon dioxide emissions associated with the reaction.[18, 19]

The vast majority of hydrogen is currently produced using fossil fuels, mostly natural gas. Overall, less than 0.7% of current hydrogen production utilizes renewable energy.[20] The production cost of green hydrogen must significantly decrease for it to be competitive with more mature carbon-based pathways of energy production.[21] In 2022, the Legislature created a sales tax exemption for the purchase of certain machinery and equipment used in the production and handling of green hydrogen.[22]

*Renewable Natural Gas*

Renewable natural gas (RNG) is the gaseous product of the decomposition of organic matter, processed into a pipeline-quality gas that is fully interchangeable with conventional natural gas. Primary sources of RNG include landfills, livestock operations, and wastewater treatment facilities.[23]

In 2021, the Legislature added the term "renewable natural gas" to Florida law and defined it as "anaerobically generated biogas, landfill gas, or wastewater treatment gas refined to a methane content of 90 percent or greater which may be used as a transportation fuel or for electric generation or is of a quality capable of being injected into a natural gas pipeline." The legislation authorizes the PSC to approve cost recovery for the purchase of RNG by natural gas public utilities, even if pricing exceeds the current market price of natural gas, if the PSC deems the purchase to be reasonable and prudent.[24] The law does not indicate what the PSC must consider in determining the reasonableness and prudence of an above-market RNG purchase.

[15] Grey hydrogen is traditionally produced from methane that is split with steam into carbon dioxide and hydrogen.
[16] Blue hydrogen production follows the same process as grey hydrogen production, but also includes the technology necessary to capture the carbon dioxide produced when hydrogen is split from methane.
[17] Despite the colorful names used for the different ways hydrogen is produced, the gas itself is invisible to the human eye. National Grid, *Energy Explained – Hydrogen Colour Spectrum*, https://www.nationalgrid.com/stories/energy-explained/hydrogen-colour-spectrum (last visited Mar. 19, 2023)
[18] Rachel Meidl & Kenneth Medlock, *The Advanced Carbon Economy: A Sustainable Hydrogen Pathway*, Rice University's Baker Institute for Public Policy, Jun. 22, 2021, p. 3, available at https://www.bakerinstitute.org/media/files/files/ec39c09c/bi-brief-062221-ces-carbonecon-4.pdf (last visited Mar. 18, 2023).
[19] When utilizing pyrolysis to produce turquoise hydrogen, the reaction does produce a solid carbon by-product that can be used in applications ranging from construction to farming. *Id.*
[20] Florida Public Service Commission, Agency Analysis of HB 821, p. 2 (Mar. 14, 2023).
[21] Office of Energy Efficiency & Renewable Energy, *supra* note 13.
[22] S. 23, ch. 2022-97, Laws of Fla., codified at s. 212.08(7)(ppp), F.S.
[23] Office of Energy Efficiency & Renewable Energy, *Alternative Fuels Data Center – Renewable Natural Gas Production*, U.S. Department of Energy, https://afdc.energy.gov/fuels/natural_gas_renewable.html (last visited Mar. 18, 2023).
[24] Ch. 2021-178, Laws of Fla., codified at s. 366.91(2)(f) and (9), F.S.

**Effect of the Bill**

The bill allows electric and natural gas public utilities to recover through rates:

- The costs of contracts for the purchase of RNG and hydrogen, with pricing above the current market value of natural gas, if the PSC finds that the contract promotes the development or use of renewable energy resources in the state and provides fuel diversification.
- Prudently-incurred costs for RNG and hydrogen fuel infrastructure projects, including but not limited to:
    - Capital investment in projects necessary to prepare or produce RNG and hydrogen fuel for pipeline distribution and usage;
    - Capital investment in facilities, including pipelines, necessary to inject and deliver RNG and hydrogen fuel throughout this state;
    - RNG and hydrogen fuel storage facilities;
    - Operation and maintenance expenses associated with any such RNG and hydrogen fuel infrastructure projects; and
    - An appropriate return on investment consistent with the return allowed for other utility plants used to provide service to customers.

For RNG and hydrogen fuel infrastructure projects, the bill allows cost recovery through an appropriate mechanism administered by the PSC. The bill provides that the costs of these infrastructure projects deemed prudent by the PSC are not subject to disallowance or further prudence review except for fraud, perjury, or intentional withholding of key information by the public utility. The bill also provides that, for purposes of cost recovery for these infrastructure projects, RNG may include a mixture of RNG and natural gas.

The bill provides an effective date of July 1, 2023.

B. SECTION DIRECTORY:

**Section 1.** Amends s. 366.91, F.S., relating to renewable energy.

**Section 2.** Provides an effective date.

## II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

   None.

2. Expenditures:

   None.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

   None. *See* Fiscal Comments.

2. Expenditures:

   None.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

Public utilities that are permitted by the PSC to recover the costs of RNG or hydrogen fuel infrastructure projects will expand the base upon which they earn a return on investment. Owners of assets from which RNG may be produced will realize additional revenue streams.

To the extent that the cost to produce and transport renewable natural gas from an RNG infrastructure project is more expensive over a project's lifetime than the production and transport of natural gas from other sources would have been, customers of public utilities will pay higher rates than they would otherwise have paid. To the extent that the cost to produce and transport hydrogen fuel from a hydrogen fuel production infrastructure project is more expensive over a project's lifetime than the cost of fuel it replaces (e.g., natural gas), customers of public utilities will pay higher rates than they otherwise would have paid. The bill does not require a showing of net benefits to utility customers.

D. FISCAL COMMENTS:

If new RNG or hydrogen fuel infrastructure projects are subject to local property taxes, the bill may create additional revenues for the local government jurisdictions in which those facilities are located, if sited within Florida.

## III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

Not Applicable. The bill does not appear to affect county or municipal governments.

2. Other:

None.

B. RULE-MAKING AUTHORITY:

The bill does not authorize or require agency rulemaking.

C. DRAFTING ISSUES OR OTHER COMMENTS:

Currently, the fuel required by public utilities to provide service in Florida is purchased from competitive providers in an open market. The PSC determines the prudence of a utility's fuel costs largely by determining whether the utility contracted for fuel on reasonable terms based on what was known or should have been known by purchasers in the market at that time. These costs are passed through to utility customers with no markup for profit to the utility. Fuel production by a public utility is not required for the utility to provide service to its customers.

The bill allows a public utility to recover through customer rates its prudently-incurred costs for certain fuel production infrastructure, expanding the types of investments upon which a monopoly utility may earn a return through customer rates. The bill does not provide guidance for the PSC in determining whether projects of this type, which have not previously been approved for cost recovery[25] – aside from one green hydrogen pilot project included as part of a comprehensive rate case settlement – are prudent. To the extent that a project is not expected to result in benefits to customers, it is not clear whether the PSC may consider other factors that would allow it to make a prudence determination.

As drafted, the bill does not require that RNG or hydrogen infrastructure projects be sited within Florida or that the fuel produced by such projects be used in the provision of utility services in the state. The bill also does not place any limits on the volume of RNG or hydrogen fuel infrastructure projects for which

[25] In 2016, the Florida Supreme Court overturned a PSC order approving cost recovery, including a profit, for an electric utility's participation in a joint venture to produce natural gas in another state, finding that the PSC's authority to set rates extends only to costs arising from the generation, transmission, or distribution of electricity in the state and that whether "cost recovery of speculative capital investments in gas exploration and production by an electric utility is in the public interest is a policy determination that must be made by the Legislature." *Citizens of the State of Florida v Art Graham*, 191 So. 3d 897, (Fla. 2016).

cost recovery may be approved by the PSC. While it may be assumed that the PSC will consider these criteria in a prudence review, the bill could be clarified to indicate whether these criteria apply.

## IV. AMENDMENTS/COMMITTEE SUBSTITUTE CHANGES

A bill to be entitled

An act relating to renewable energy cost recovery; amending s. 366.91, F.S.; revising the types of contracts which are eligible for cost recovery by a public utility under certain circumstances; authorizing a public utility to recover prudently incurred renewable natural gas and hydrogen fuel infrastructure project costs through the appropriate Public Service Commission cost-recovery mechanism; providing that such costs prudently incurred are not subject to further actions except under certain circumstances; specifying eligible renewable natural gas and hydrogen fuel infrastructure projects; providing an effective date.

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

Section 1. Subsection (9) of section 366.91, Florida Statutes, is amended, and subsection (10) is added to that section, to read:

366.91 Renewable energy.—

(9) ~~The commission may approve cost recovery by a gas public utility for~~ Contracts for the purchase of renewable natural gas and hydrogen in which the pricing provisions exceed the current market price of natural gas are eligible for cost



CODING: Words ~~stricken~~ are deletions; words underlined are additions.

recovery, but only if ~~which are otherwise deemed reasonable and prudent by~~ the commission finds that the contract meets the overall goals of subsection (1) by promoting the development or use of renewable energy resources in this state and providing fuel diversification.

(10) A public utility may recover, through the appropriate cost-recovery mechanism administered by the commission, prudently incurred costs for renewable natural gas and hydrogen fuel infrastructure projects. If the commission determines that such costs were prudently incurred, those costs are not subject to disallowance or further prudence review except for fraud, perjury, or intentional withholding of key information by the public utility. For purposes of this subsection for utility cost recovery only, renewable natural gas may include a mixture of natural gas and renewable natural gas. Eligible renewable natural gas and hydrogen fuel infrastructure projects include, but are not limited to, capital investment in projects necessary to prepare or produce renewable natural gas and hydrogen fuel for pipeline distribution and usage; capital investment in facilities, including pipelines, necessary to inject and deliver renewable natural gas and hydrogen fuel throughout this state; renewable natural gas and hydrogen fuel storage facilities; operation and maintenance expenses associated with any such renewable natural gas and hydrogen fuel infrastructure projects; and an appropriate return on investment consistent with that

allowed for other utility plants used to provide service to customers.

Section 2. This act shall take effect July 1, 2023.

# Energy, Communications & Cybersecurity Subcommittee
# HB 821 by Rep. Yeager
# Renewable Energy Cost Recovery

## AMENDMENT SUMMARY
## March 21, 2023

---

**Amendment 1 by Rep. Yeager (strike-all):**

- Specifies factors that the Public Service Commission (PSC) may consider in determining whether a public utility contract for the purchase of renewable natural gas (RNG) or hydrogen fuel is in the public interest.
- Specifies factors that the Public Service Commission (PSC) must consider in determining whether a public utility's RNG or hydrogen fuel infrastructure project is in the public interest.
- Clarifies that an eligible RNG or hydrogen fuel infrastructure project must be located in Florida.
- Specifies that costs incurred by a public utility for an RNG or hydrogen fuel infrastructure project approved for cost recovery shall not be allowed until the facility is placed in service.
- Requires an annual report from the PSC to provide information related to approved RNG and hydrogen fuel infrastructure projects.
- Provides for repeal on June 30, 2028, unless reviewed and saved by the Legislature; allows for continued recovery of previously approved costs after the repeal date.

COMMITTEE/SUBCOMMITTEE ACTION

| | | |
|---|---|---|
| ADOPTED | ___ | (Y/N) |
| ADOPTED AS AMENDED | ___ | (Y/N) |
| ADOPTED W/O OBJECTION | ___ | (Y/N) |
| FAILED TO ADOPT | ___ | (Y/N) |
| WITHDRAWN | ___ | (Y/N) |
| OTHER | _____ | |

Committee/Subcommittee hearing bill: Energy, Communications & Cybersecurity Subcommittee
Representative Yeager offered the following:

**Amendment (with title amendment)**

Remove everything after the enacting clause and insert:

Section 1. Subsection (9) of section 366.91, Florida Statutes, is amended, and subsection (10) is added to that section, to read:

366.91 Renewable energy.—

(9) ~~The commission may approve cost recovery by a gas public utility for~~ A public utility contract~~s~~ for the purchase of renewable natural gas or hydrogen fuel in which the pricing provisions exceed the current market price of natural gas is eligible for cost recovery, but only if ~~which are otherwise deemed reasonable and prudent by~~ the commission finds, that the

contract provides net benefits to the public utility and its customers and is therefore in the public interest. In making this determination, the commission may consider the contract's impact on the overall diversity of the public utility's natural gas commodity supply or other fuel supply, the potential to reduce the impact of volatility in the natural gas commodity market upon the public utility and its customers, any reliability benefits associated with the in-state production of these fuel supplies, and the public utility's cost of fuel.

(10)(a) A public utility may petition the commission for approval to recover costs prudently incurred for a renewable natural gas or hydrogen fuel infrastructure project at a location in Florida for use in providing utility service within this state.

(b) In its review of a petition filed pursuant to this subsection, the commission shall consider:

1. The estimated volume and reliability of renewable natural gas or hydrogen fuel that the project will produce for use by the public utility, and the comparative cost of the same volume of volume of natural gas purchases;

2. The estimated rate impact of the project over time, including estimated savings, if any, to the public utility and its customers;

3. The service and reliability benefits to be derived from the project;

4. The proposed mechanism for recovery of project costs;

5. The impact of the project on fuel diversity in this state and fuel cost volatility; and

6. Any other matter deemed relevant by the commission.

(c)1. Upon consideration of all matters specified in paragraph (b), the commission shall determine whether, and the extent to which, approval for recovery of project costs from the public utility's ratepayers provides net benefits to the state and is therefore in the public interest.

2. If the commission approves recovery of project costs, in whole or in part, the commission shall determine the appropriate mechanism for recovery of such costs. Appropriate mechanisms may include an existing cost recovery mechanism, not excluding base rates, or a new cost recovery mechanism established by the commission.

3. Costs approved by the commission are not subject to disallowance or further prudence review except for fraud, perjury, or intentional withholding of material information by the public utility.

(d) Costs of renewable natural gas and hydrogen fuel infrastructure projects that are eligible for recovery under this subsection include:

1. Capital investment in projects necessary to prepare or produce renewable natural gas or hydrogen fuel for pipeline distribution and usage;

2. Capital investment in facilities, including pipelines, necessary to inject into pipelines, and deliver for utility use, renewable natural gas or hydrogen fuel throughout this state;

3. Renewable natural gas and hydrogen fuel storage facilities;

4. Operation and maintenance expenses associated with such renewable natural gas and hydrogen fuel infrastructure projects; and

5. An appropriate return on investment consistent with the utility's authorized return on investment for other utility plants used to provide service to customers.

(e) Recovery of costs incurred by a public utility for a renewable natural gas or hydrogen fuel infrastructure project approved for cost recovery under this section shall not be allowed until such facility is placed in service. Upon approval of cost recovery by the commission, costs incurred prior to the facility being placed in service may be deferred on the public utility's books for recovery once the facility is in service. This shall not preclude application of any other appropriate regulatory accounting rules that are otherwise deemed appropriate, including but not limited to, normal recovery of costs for construction work in progress.

(f) Beginning January 1, 2025, the commission must annually submit a report to the Governor, the President of the Senate, and the Speaker of the House of Representatives

indicating, for the 12-month reporting period and cumulatively: the investment made in such infrastructure projects; the eligible costs incurred and the amount of such costs recovered; the volume of renewable natural gas or hydrogen fuel used to provide utility service; and an analysis of the price of renewable natural gas or hydrogen fuel used to provide utility service as compared to the market cost of gas, including actual rate impacts of such projects.

(g) This subsection shall stand repealed on June 30, 2028, unless reviewed and saved from repeal by the Legislature. A public utility may continue to recover eligible costs of renewable natural gas or hydrogen fuel infrastructure projects approved prior to June 30, 2028, under this subsection as being in the public interest.

(h) The commission may adopt rules to implement and administer this section.

---

**T I T L E A M E N D M E N T**

Remove everything before the enacting clause and insert: An act relating to renewable energy cost recovery; amending s. 366.91, F.S.; revising the types of contracts which are eligible for cost recovery by a public utility under certain circumstances; authorizing a public utility to recover prudently

incurred renewable natural gas and hydrogen fuel infrastructure project costs approved by the Public Service Commission; establishing criteria for consideration by the Public Service Commission; establishing terms for cost recovery; specifying eligible renewable natural gas and hydrogen fuel infrastructure projects; requiring an annual report; providing for repeal on June 30, 2028, unless reviewed and saved from repeal by the Legislature; providing an effective date.

# HB 1221

# HOUSE OF REPRESENTATIVES STAFF ANALYSIS

**BILL #:** HB 1221 Broadband Internet Service Providers
**SPONSOR(S):** Tomkow
**TIED BILLS:** **IDEN./SIM. BILLS:** CS/SB 626

| REFERENCE | ACTION | ANALYST | STAFF DIRECTOR or BUDGET/POLICY CHIEF |
|---|---|---|---|
| 1) Energy, Communications & Cybersecurity Subcommittee | | Keating | Keating |
| 2) State Administration & Technology Appropriations Subcommittee | | | |
| 3) Commerce Committee | | | |

## SUMMARY ANALYSIS

Rural electric cooperatives are electric utilities owned by their customer-members and located primarily in rural areas where, at least historically, the economics of building or installing electrical infrastructure has not attracted investment. To promote economic development, a cooperative in Florida may provide any energy or nonenergy services to its membership. Currently, five of Florida's 18 rural electric cooperatives are engaged in or developing broadband service for their members. Both the state and federal government offer grant funds to entities seeking to expand broadband Internet service into unserved areas.

The term pole attachment refers to the process by which communications services providers can place communications infrastructure on existing electric utility poles. Rules governing pole attachments seek to balance the desire to maximize value for users of both electric and communications services with concerns unique to electric utility poles, such as safety and reliability. Since 2021, the Public Service Commission (PSC) has had the authority to regulate and enforce rates, charges, terms, and conditions for pole attachments to ensure that they are just and reasonable. No party yet has initiated proceedings at the PSC under this authority. Attachments to poles owned by rural electric cooperatives are, and have historically been, exempt from regulation.

The bill provides explicit authority for rural electric cooperatives in Florida to provide specified communications services in the following circumstances:

- The cooperative provides broadband Internet service directly or in partnership with a third party; or
- The cooperative receives broadband grant funding pursuant to the Florida Broadband Opportunity Program or from any other federal or state program offering grants to expand broadband Internet service to unserved areas of the state.

Under the bill, if a cooperative provides a communications service under these terms, all poles owned by the cooperative are subject to the PSC's pole attachment regulations on the same terms as poles owned by investor-owned electric utilities. Thus, the financial and legal responsibilities of parties to rural electric cooperative pole attachment arrangements may substantially change depending on the PSC's implementation of its authority over pole attachment rates, charges, terms, and conditions.

The bill does not impact state or local government revenues or local government expenditures. The bill may increase state government expenditures, but the PSC has indicated that it can handle the expected increased workload with existing resources.

The bill provides an effective date of July 1, 2023.

## FULL ANALYSIS

## I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

**Current Situation**

Regulation of Pole Attachments

The term pole attachment refers to the process by which communications services providers can place communications infrastructure on existing electric utility poles. This reduces the number of poles that must be built to accommodate utility and communications services, while reducing costs to users of both services by allowing providers to share costs. Rules governing pole attachments seek to balance the desire to maximize value for users of both electric and communications services with concerns unique to electric utility poles, such as safety and reliability.[1] The space requested for a pole attachment is typically one foot.

Pole attachments, originally by mutual agreement but later by federal statute and regulation, provide non-pole-owning cable and telecommunication service providers with access to a utility's distribution poles, conduits, and ROW for:

- Installing fiber, coaxial cable or wires, and other equipment;
- Building an interconnected network; and
- Reaching customers.[2]

Congress began regulating pole attachments[3] in 1978.[4] The Telecommunications Act of 1996[5] (the Act) expanded pole attachment rights to telecommunications[6] carriers. The Act requires utilities[7] to provide nondiscriminatory access to cable television systems and telecommunications carriers. The Act also authorizes the Federal Communications Commission[8] (FCC) to regulate the rates, terms, and conditions of attachments by cable television operators to the poles, conduit, or ROW owned or controlled by utilities in the absence of parallel state regulation.[9] The Legislation withheld from FCC jurisdiction the authority to regulate attachments where the utility is a railroad, cooperatively organized, or owned by a government entity.[10] Thus, federal pole attachment regulations apply only to investor-owned electric utilities (IOUs). Municipal and cooperative electric utilities are specifically exempted from federal pole attachment regulations.

The Act permits utilities to deny access where there is insufficient capacity and for reasons of safety, reliability or generally applicable engineering purposes. In addition to establishing a right of access, the Act provides a rate methodology for "attachments used by telecommunications carriers to provide

[1] American Public Power Association, *Issue Brief: Preserving the Municipal Exemption from Federal Pole Attachment Regulations* (Jan. 2021) https://www.publicpower.org/policy/preserving-municipal-exemption-federal-pole-attachment-regulations (last visited Mar. 13, 2021).
[2] Edison Electric Institute, Pole Attachments 101, https://ecfsapi.fcc.gov/file/7020708245.pdf (last visited Mar. 13, 2021).
[3] 47 U.S.C. § 224(a)(4), defines ''pole attachment'' as "any attachment by a cable television system or provider of telecommunications service to a pole, duct, conduit, or right-of-way owned or controlled by a utility."
[4] The Pole Attachment Act of 1978 granted utility pole access to cable companies, and was designed to promote utility competition and service to the public. Communications Act Amendments of 1978, Pub. L. No. 95-234. (Feb. 21, 1978).
[5] Telecommunications Act of 1996, Pub. LA. No. 104-104, 110 Stat. 56 (1996).
[6] The term "telecommunications" means the transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received. 47 U.S.C. § 153(50).
[7] 47 U.S.C. § 224(a)(1), defines ''utility'' as "any person who is a local exchange carrier or an electric, gas, water, steam, or other public utility, and who owns or controls poles, ducts, conduits, or rights-of-way used, in whole or in part, for any wire communications. Such term does not include any railroad, any person who is cooperatively organized, or any person owned by the Federal Government or any State."
[8] The FCC regulates interstate and international communications by radio, television, wire, satellite and cable in all 50 states, the District of Columbia and U.S. territories. An independent U.S. government agency overseen by Congress, the FCC is the United States' primary authority for communications law, regulation and technological innovation. FCC, *What We Do*, https://www.fcc.gov/about-fcc/what-we-do (last visited Mar 19, 2023).
[9] 47 U.S.C. § 224.
[10] *In the Matter of Implementation of Section 224 of the Act- A Nat'l Broadband Plan for Our Future*, 26 F.C.C. Rcd. 5240, 5245–46 (2011)

telecommunications services"[11] in addition to the existing methodology for attachments "used by a cable television system solely to provide cable service.[12]

Federal law broadly preempts the regulation of telecommunications services.[13] However, federal law allows states to exercise reverse preemption over the FCC's jurisdiction of communications infrastructure access,[14] meaning that once a state adopts its own utility pole access rules, the FCC loses jurisdiction over pole attachments to the extent that the state regulates such matters.[15]

Pursuant to section 224(c) of the Act[16], each state that regulates the rates, terms, and conditions for pole attachments must certify to the FCC that:

- It regulates such rates, terms, and conditions; and
- In so regulating such rates, terms, and conditions, the state has the authority to consider and does consider the interests of the subscribers of the services offered via such attachments, as well as the interests of the consumers of the utility services provided by the pole owners.

Furthermore, a state is not considered to regulate the rates, terms, and conditions for pole attachments:

- Unless the state has issued and made effective rules and regulations implementing the state's regulatory authority over pole attachments; and
- With respect to any individual matter, unless the state takes final action on a complaint regarding such matter:
    - Within 180 days after the complaint is filed with the state, or
    - Within the applicable period prescribed for such final action in such rules and regulations of the state, if the prescribed period does not extend beyond 360 days after the filing of such complaint.

*In Florida*

In 2021, Florida exercised its power under the Act to assert reverse preemption over the FCC's regulation of pole attachments, directing the Florida Public Service Commission (PSC) to regulate and enforce rates, charges, terms, and conditions for pole attachments, and to ensure that they are just and reasonable. Accordingly, Florida law requires the PSC to adopt rules to administer its new regulatory authority and, in doing so, to consider the interests of the subscribers and users of the services offered through pole attachments, as well as the interests of the consumers of any pole owner providing such attachments.[17] Florida law maintains the federal regulatory exemption for attachments to poles owned by government-owned or cooperative electric utilities.

Florida law provides that the Legislature's intent is to encourage parties to enter into voluntary pole attachment agreements and provides that it may not be construed to prevent parties from voluntarily entering into such agreements without PSC approval. The law requires the PSC to hear and resolve complaints concerning rates, charges, terms, conditions, voluntary agreements, or any denial of access relative to pole attachments. The law specifies that a party's right to nondiscriminatory access to a pole is identical to the rights afforded under section 224(f)(1) of the Act,[18] and that a pole owner may deny access to its poles on a nondiscriminatory basis when there is insufficient capacity, for reasons of safety and reliability, and when required by generally applicable engineering purposes. A pole owner must consider relevant construction and reliability standards approved by the PSC when evaluating capacity, safety, reliability, and engineering requirements.

---

[11] 47 U.S.C. § 224(e).
[12] 47 U.S.C. § 224(d).
[13] "No State or local statute or regulation, or other State or local legal requirement, may prohibit or have the effect of prohibiting the ability of any entity to provide any interstate or intrastate telecommunications service." 47 U.S.C. § 253(a).
[14] 47 U.S.C. § 224(c)(1).
[15] Catherine J.K. Sandoval, *Contested Places, Utility Pole Spaces: A Competition and Safety Framework for Analyzing Utility Pole Association Rules, Roles, and Risks*, 69 Cath. U. L. Rev. 473, 486–87 (2020).
[16] 47 U.S.C. § 224(c)
[17] Ch. 2021-191, Laws of Fla., codified at s. 366.04(8), F.S.
[18] 47 U.S.C. s. 224(f)(1) provides for nondiscriminatory access to any pole, duct, conduit, or right-of-way owned or controlled by a utility, subject to denial, on a nondiscriminatory basis, only on the grounds of insufficient pole capacity or for safety, reliability, or other engineering purposes.

Under Florida law, FCC precedent is not binding upon the PSC. However, the bill requires the PSC to apply the decisions and orders of the FCC and related appellate court decisions when determining just and reasonable pole attachment rates, terms and conditions unless a pole owner or attaching entity establishes by competent substantial evidence that an alternative cost-of-service based pole attachment rate is appropriate and in the public interest.

To help establish precedent on the establishment of pole attachment rates and guide negotiations toward voluntary pole attachment agreements, Florida law authorizes any pole owner or attaching entity to participate in the first five formal administrative proceedings conducted by the PSC to determine pole attachment rates. After the fifth such formal administrative proceeding is concluded by final order, parties to subsequent pole attachment rate proceedings are limited to the specific pole owner and pole attaching entities involved in and directly affected by the specific pole attachment rate. Currently, no party has initiated a pole attachment proceeding at the PSC.

Rural Electric Cooperatives

Rural electric cooperatives are electric utilities that are owned by their consumer-members. These private companies are generally nonprofit, with their principal purpose being to deliver electrical service to their members. Rural electric cooperatives are mostly located in rural areas where, at least historically, the return on investment for building or installing electrical infrastructure was not enough for investor-owned utilities to want to service them.[19]

Historically, rural homes, farms, and businesses were some of the last places to electrify in the United States (U.S.). By the mid-1930's, 90 percent of U.S. urban homes were electrified,[20] however, the opposite was true in rural areas—only one out of 10 rural homes had electric service.[21] This lack of electrical service deeply limited economic development in rural areas of the country. Despite this impact, the costs to electrify most rural areas were usually prohibitive and often thought not economically feasible.[22] In the limited areas where rural electric power was available, often the prices paid by such consumers were far higher than those paid by their urban counterparts.

In 1935, Executive Order 7037, issued by President Franklin Roosevelt, created the Rural Electrification Administration (REA). One year later, Congress passed the Rural Electrification Act (Pub. L. 74–605), codifying the REA and creating a loan program to encourage the growth of rural electrification. Even with these available federal loans, established investor-owned utilities did not have much interest in building rural systems. However, there was significant interest from farmer-based electric cooperatives.[23] By 1939, with assistance from REA funds, 413 rural electric cooperatives had been established in the U.S.,[24] and by 1950, 80 percent of U.S. farms had electric service.[25]

During a reorganization of the United States Department of Agriculture (USDA) in 1994, the REA was replaced with the Rural Utilities Service, which still exists today.[26] According to the National Rural Electric Cooperative Association (NRECA), now over 99 percent of U.S. farms have electrical service.[27] Rural electric cooperatives continue to be the most prevalent way for consumers in rural areas to obtain electrical service.[28]

[19] University of Wisconsin Center for Cooperatives, *Research on the Economic Impact of Cooperatives*, https://reic.uwcc.wisc.edu/electric/ (last visited Mar. 19, 2023).
[20] *Id.*
[21] National Rural Electric Cooperative Association, *History,* https://www.electric.coop/our-organization/history (last visited Mar. 19, 2023).
[22] United States Department of Agriculture, *Celebrating the 80th Anniversary of the Rural Electrification Administration*, Feb. 21, 2017, https://www.usda.gov/media/blog/2016/05/20/celebrating-80th-anniversary-rural-electrification-administration (last visited Mar.19, 2023).
[23] National Rural Electric Cooperative Association, *History, supra* note 22.
[24] University of Wisconsin Center for Cooperatives, *supra* note 20.
[25] *Celebrating the 80th Anniversary of the Rural Electrification Administration, supra* note 23.
[26] University of Wisconsin Center for Cooperatives, *supra* note 20.
[27] National Rural Electric Cooperative Association, *History, supra* note 22.
[28] United States Energy Information Administration, *Today in Energy: August 15, 2019*, https://www.eia.gov/todayinenergy/detail.php?id=40913.

As of 2019, rural electric cooperatives in the U.S. averaged 7.98 customers per mile of line, as compared with 32.4 customers per mile of line for the rest of the electricity industry. In addition, while rural electric cooperatives have ownership of 42 percent of U.S. electricity distribution lines, their electricity sales only represent 12 percent of the nation's overall sales. Rural electric cooperatives have a different customer mix as well. For rural electric cooperatives, 53 percent of their customers are residential, with the remainder being commercial, industrial, and transportation customers—which generally have much higher energy consumption. For the U.S. electric industry at-large, the percentage of residential customers is 38 percent.[29]

These factors lead to rural electric cooperatives receiving significantly less revenue per dollar of capital investment in distribution. Rural electric cooperatives' average revenue for mile of distribution line is $19,135 (versus $79,298 for the rest of the electricity industry) and their cost of distribution plant per customer is $4,219 (versus $3,698).[30] Thus, on a per customer basis, the distribution of electric power in rural areas is higher versus the rest of the industry.

*In Florida*

In 1937, the REA drafted the Electric Cooperative Corporation Act as a model state law for states to adopt for forming and operating rural electric cooperatives. Florida's first distribution electric cooperatives were formed that same year.[31] At that time, much of Florida's geographic territory lacked electrical service, due to, like most of the U.S., the lack of enough economic development to make providing service worthwhile for existing electric companies.

At present, Florida has 18 rural electric cooperatives, with 16 of these cooperatives being distribution cooperatives and two being generation and transmission cooperatives. These cooperatives are represented by the Florida Electric Cooperative Association (FECA).[32] These cooperatives operate in 57 of Florida's 67 counties and have more than 2.7 million customers.[33] Much like other areas of the U.S., Florida rural electric cooperatives serve a large percentage of area, but have a low customer density. Specifically, Florida cooperatives serve approximately 10 percent of Florida's total electric utility customers, but their service territory covers 60 percent of Florida's total land mass. Each cooperative is governed by a board of cooperative members elected by the cooperative's membership.[34]

In addition to providing electric service, cooperatives in Florida are authorized to own and operate water and sewer systems.[35] To promote economic development, cooperatives may provide any energy or nonenergy services to its membership.[36]

Broadband Internet Deployment

Fixed and mobile broadband Internet services provide access to numerous employment, education, entertainment, and health care opportunities.[37] Communities that lack broadband access can have difficulty attracting new capital investment. While Florida's urban areas are served at a fixed broadband coverage rate of 98 percent, its rural areas are served at a rate of 78.6 percent.[38] This disparity is caused primarily by high per-unit construction costs required to build broadband infrastructure across

[29] National Rural Electric Cooperative Association, *Fact Sheet: February 2021*, https://www.cooperative.com/programs-services/bts/documents/data/electric-co-op-fact-sheet-update-february-2021.pdf (last visited Mar. 19, 2023).
[30] *Id.*
[31] Seminole Electric Cooperative, *Empowering our Community*, https://www.seminole-electric.com/ (last visited Mar. 19, 2023).
[32] Florida Electric Cooperative Association, *Members*, https://feca.com/members/ (last visited Mar 19, 2023).
[33] Florida Electric Cooperative Association, *Our History*, https://feca.com/our-history/ (last visited Mar 19, 2023).
[34] *Id.*
[35] S. 425.04(4), F.S.
[36] S. 425.04 (15), F.S.
[37] U.S. Federal Communications Commission (FCC), *2018 Broadband Deployment Report,* at 1 (Feb. 2, 2018), *available at* https://docs.fcc.gov/public/attachments/FCC-18-10A1.pdf (last visited Mar. 23, 2023).
[38] FCC, *2021 Broadband Deployment Report* at 63 (Jan. 19, 2021), *available at* https://docs.fcc.gov/public/attachments/FCC-21-18A1.pdf (last visited Mar. 23, 2023). For purposes of this data, 'fixed broadband services' are measured at 25 megabits per second downstream and 3 megabits per second upstream.

larger swaths of rural geographic areas.[39] The recent COVID-19 pandemic amplified the need for broadband Internet access in everyday life. Studies indicate that broadband Internet access matters for jobs, income, business relocation, civic engagement, and health.[40]

*Broadband Growth Programs*

- Florida Broadband Opportunity Program

Established under s. 288.9962, F.S., the Broadband Opportunity Program (BOP) is a competitive reimbursement program within the Florida Department of Economic Opportunity (DEO).[41] The purpose of the program is to award grants to applicants who seek to expand broadband Internet service to unserved areas of Florida. To operate the program, the Legislature appropriated $400 million in federally funded State and Local Fiscal Recovery Funds (SLFRF) to increase Floridians' access to reliable, affordable, and high-speed internet service.[42]

- Connect America Fund

One of the earliest and most significant federal broadband programs is the Connect America Fund, which is part of the FCC's Universal Service Fund (USF). Started in 2011, the purpose of the fund is to provide subsidies to telecommunications companies to expand telecommunications infrastructure in rural and remote areas of the United States.[43] The Connect America Fund is a "high-cost" program, meaning that it is designed to ensure that consumers in rural, insular, and high cost areas have access to modern telecommunications networks and that services through those networks, like voice and broadband, are available at a cost comparable to that in more developed urban areas.[44] The Connect America Fund is the largest of the USF's programs, and has an annual budget of $4.5 billion.[45]

- Broadband Technology Opportunities Program

The Broadband Technology Opportunities Program (BTOP) is a federal grant program administered by the National Telecommunications and Information Administration (NTIA), part of the U.S. Department of Commerce. The BTOP is funded by the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5), and has an annual budget of $4 billion. The purpose of the program is to "bridge the technological divide" and BTOP projects include deploying broadband Internet infrastructure, enhancing and expanding public computer centers, and encouraging the sustainable adoption of broadband service.[46]

- USDA Programs: ReConnect Program and the Rural Broadband Program

The USDA operates two programs aimed at developing broadband in rural areas—the ReConnect Program and the Rural Broadband Program. Though these programs both existed prior to 2021, the Infrastructure Investment and Jobs Act (Public Law 117-58), signed into law on November 15, 2021,

[39] American Broadband Initiative, *Milestones Report*, at 11 (Feb. 13, 2019), *available at* https://www.ntia.doc.gov/files/ntia/publications/american_broadband_initiative_milestones_report.pdf (last visited Mar. 23, 2023).
[40] *COVID-19 lockdowns expose the digital have-nots in rural areas – here's which policies can get them connected* (Sep. 2, 2020), https://theconversation.com/covid-19-lockdowns-expose-the-digital-have-nots-in-rural-areas-heres-which-policies-can-get-them-connected-144324 (last visited Mar. 23, 2023).
[41] Florida Department of Economic Opportunity, *Broadband Opportunity Program*, https://www.floridajobs.org/community-planning-and-development/broadband/broadband-opportunity-program (last visited Mar. 19, 2023).
[42] *Id.*
[43] Federal Communications Commission, *Universal Service Monitoring Report*, Feb. 13, 2023, (available at: https://www.fcc.gov/general/federal-state-joint-board-monitoring-reports).
[44] Federal Communications Commission, *Universal Service for High Cost Areas-Connect America Fund,* https://www.fcc.gov/general/universal-service-high-cost-areas-connect-america-fund#releases (last visited Mar. 19, 2023).
[45] Universal Service Administrative Co., *Program Overview*, https://www.usac.org/high-cost/program-overview/ (last visited Mar 3, 2023).19
[46] National Telecommunications and Information Administration, *Broadband Technology Opportunities Program,* https://ntia.gov/category/broadband-technology-opportunities-program#:~:text=The%20Broadband%20Technology%20Opportunities%20Program,in%20communities%20across%20the%20country (last visited Mar. 19, 2023).

provided new funding for both of these programs (and other broadband initiatives). The ReConnect Program received $1.926 billion in funds for grants and loans and the Rural Broadband Program received $74 million in funds for loans.[47]

The purpose of the ReConnect Program is to offer loans, grants, and loan-grant combinations to facilitate broadband deployment in rural areas that currently do not have sufficient access to broadband. The entities eligible to apply for the Reconnect Program include:

- Corporations, limited liability companies, and limited liability partnerships;
- State and local governments;
- U.S. territories and possessions; and
- Indian tribes, as defined in Section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. §450b).48

Reconnect grants may be used for:

- Construction or improvement of facilities required to provide fixed terrestrial broadband services;
- Funding of reasonable pre-application expenses; and
- Funding the acquisition of an existing telecommunications system that does not currently provide sufficient access to broadband.[49]

The Rural Broadband Program offers funds to help construct, improve, or acquire facilities and equipment needed to provide broadband to rural areas. The entities eligible to apply for the program are:

- Corporations
- Limited liability companies
- Cooperative or mutual organizations
- State and local governments
- Indian tribes and tribal organizations

For the most recent years prior to 2021, Congress only appropriated funds to the Rural Broadband Program for loans. However, with the increase in funding under the Infrastructure Investment and Jobs Act, funding for grants and loan guarantees is also now available in the program.[50]

While the USDA's Reconnect and Rural programs are similar in their purpose, a key distinction lies in the standards for eligible service areas. For the ReConnect Program, eligible service areas exist where at least 90% of households lack sufficient access to broadband with at least 100 Mbps download and 20 Mbps upload speed (100/20 Mbps service). For the Rural Broadband Program, the standard for eligibility is if the area in question does not have at least 50% of households with at least 25 Mbps download and 3 Mbps upload speed (25/3 Mbps service).

*Rural Electric Cooperative Engagement in Broadband*

According to the NRECA, about 200 rural electric cooperatives are currently providing or building out broadband service. In addition, the NRECA states that 200 additional rural electric cooperatives are "assessing the feasibility of providing service to more than 6 million households in co-op service areas that don't have access to high-speed internet service."[51] To support its members who are or would like to be engaged in the broadband business, the NRECA launched a new level of service for its members in July 2022 called NRECA Broadband.[52] The stated purpose of NRECA Broadband is to offer federal

[47] Congressional Research Service, *Infrastructure Investment and Jobs Act: Funding for USDA Rural Broadband Programs*, Nov. 19. 2021 (available at: https://crsreports.congress.gov/product/pdf/IF/IF11918).
[48] United States Department of Agriculture, *ReConnect Program*, https://www.usda.gov/reconnect/program-overview (last visited Mar 19, 2023).
[49] *Id.*
[50] Federal Communications Commission, *Universal Service for High Cost Areas-Connect America Fund,* supra note 47.
[51] National Rural Electric Cooperatives Association, *Broadband,* https://www.electric.coop/issues-and-policy/broadband (last visited Mar 19, 2023).
[52] *Id.*

policy and regulatory advocacy; communication, events, and education; and operations and technology support.[53]

While rural electric cooperatives have experience in operating a monopoly electric utility, many have little institutional experience in operating in a non-monopoly competitive market in general or in broadband telecommunications specifically. Thus, these companies can face challenges in learning how to market and provide broadband services.[54]

Currently, five of Florida's 18 rural electric cooperatives, are engaged in or developing broadband service:

- Glades Electric Cooperative (5.1 members per mile of line).
- Central Florida Electric Cooperative (6.34 members per mile of line).
- Suwannee Valley Electric Cooperative (4.5 members per mile of line).
- Tri-County Electric Cooperative (4.48 members per mile of line).
- Escambia River Electric Cooperative (6.94 members per mile of line).

According to the FECA these five cooperatives are the most rural in nature of the cooperatives in Florida.[55]

**Effect of the Bill**

The bill explicitly authorizes rural electric cooperatives in Florida to provide communications services, as defined in s. 350.81, F.S., in the following circumstances:

- The cooperative provides broadband service directly or in partnership with a third party; or
- The cooperative receives broadband grant funding pursuant to the Florida Broadband Opportunity Program or from any other federal or state program offering grants to expand broadband Internet service to unserved areas of the state.

Communications services, as defined in s. 350.81, F.S., include any advanced service, cable service, or telecommunications service. Advanced service includes high-speed-Internet-access-service capability in excess of 200 kilobits per second in the upstream or the downstream direction.[56]

If a cooperative provides a communications service under these terms, all poles owned by the cooperative are subject to pole attachment regulation on the same terms as poles owned by investor-owned electric utilities.

B. SECTION DIRECTORY:

**Section 1.** Amends s. 425.04, F.S., relating to powers of rural electric cooperatives.

**Section 2.** Provides an effective date.

## II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

None.

[53] Cooperative.com, *NRECA Broadband*, https://www.cooperative.com/topics/telecommunications-broadband/nreca-broadband/Pages/default.aspx (last visited Mar. 19, 2023).
[54] National Rural Electric Cooperatives Association, *Along Those Lines: What It Takes for Electric Co-ops to Enter the Broadband Space*, Jan 24, 2023, https://www.electric.coop/along-those-lines-what-it-takes-for-electric-co-ops-to-enter-the-broadband-space.
[55] Senate Analysis of CS/SB 626 (2023), p. 15 (March 8, 2023), citing an email from Drew Love, Director of Government Affairs, Florida Electric Cooperatives Association, to Senate Regulated Industries Staff (Mar. 6, 2023).
[56] S. 350.81, F.S.

2. Expenditures:

The bill may increase state government expenditures. The PSC has indicated that it can handle the expected increased workload with existing resources.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

None.

2. Expenditures:

None.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

The financial and legal responsibilities of parties to rural electric cooperative pole attachment arrangements in Florida may substantially change depending on the PSC's implementation of new pole attachment regulatory authority under this bill.

D. FISCAL COMMENTS:

None.

## III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

Not Applicable. The bill does not appear to affect county or municipal governments.

2. Other:

None.

B. RULE-MAKING AUTHORITY:

The bill does not authorize or require agency rulemaking.

C. DRAFTING ISSUES OR OTHER COMMENTS:

None.

## IV. AMENDMENTS/COMMITTEE SUBSTITUTE CHANGES

A bill to be entitled

An act relating to broadband Internet service providers; amending s. 425.04, F.S.; authorizing rural electric cooperatives to provide communications services under certain circumstances for the purpose of expanding broadband Internet service to unserved areas of this state; providing an effective date.

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

Section 1. Section 425.04, Florida Statutes, is amended, to read:

425.04 Powers.—A cooperative shall have all of the following powers ~~power~~:

(1) To sue and be sued, in its corporate name.~~;~~

(2) To have perpetual existence.~~;~~

(3) To adopt a corporate seal and alter the same at pleasure.~~;~~

(4) To generate, manufacture, purchase, acquire, accumulate and transmit electric energy, and to distribute, sell, supply, and dispose of electric energy in rural areas to its members, to governmental agencies and political subdivisions, and to other persons not in excess of 10 percent of the number of its members; to process, treat, sell, and dispose of water and water rights; to purchase, construct, own

and operate water systems; to own and operate sanitary sewer systems; and to supply water and sanitary sewer services. However, a ~~no~~ cooperative may not ~~shall~~ distribute or sell any electricity, or electric energy to any person residing within any town, city or area in which the person is receiving adequate central station service or who at the time of commencing such service, or offer to serve, by a cooperative, is receiving adequate central station service from any utility agency, privately or municipally owned individual partnership or corporation.~~;~~

(5) To make loans to persons to whom electric energy is or will be supplied by the cooperative for the purpose of, and otherwise to assist such person in, wiring their premises and installing therein electric and plumbing fixtures, appliances, apparatus and equipment of any and all kinds and character, and in connection therewith, to purchase, acquire, lease, sell, distribute, install and repair such electric and plumbing fixtures, appliances, apparatus and equipment, and to accept or otherwise acquire, and to sell, assign, transfer, endorse, pledge, hypothecate and otherwise dispose of notes, bonds and other evidences of indebtedness and any and all types of security therefor.~~;~~

(6) To make loans to persons to whom electric energy is or will be supplied by the cooperative for the purpose of, and otherwise to assist such persons in, constructing, maintaining

and operating electric refrigeration plants.~~;~~

(7) To become a member in one or more other cooperatives or corporations or to own stock therein.~~;~~

(8) To construct, purchase, take, receive, lease as lessee, or otherwise acquire, and to own, hold, use, equip, maintain, and operate, and to sell, assign, transfer, convey, exchange, lease as lessor, mortgage, pledge, or otherwise dispose of or encumber, electric transmission and distribution lines or systems, electric generating plants, electric refrigeration plants, lands, buildings, structures, dams, plants and equipment, and any and all kinds and classes of real or personal property whatsoever, which shall be deemed necessary, convenient or appropriate to accomplish the purpose for which the cooperative is organized.~~;~~

(9) To purchase or otherwise acquire; to own, hold, use and exercise; and to sell, assign, transfer, convey, mortgage, pledge, hypothecate, or otherwise dispose of or encumber, franchises, rights, privileges, licenses, rights-of-way and easement.~~;~~

(10) To borrow money and otherwise contract indebtedness; to issue notes, bonds, and other evidences of indebtedness therefor; and to secure the payment thereof by mortgage, pledge, deed of trust, or any other encumbrance upon any or all of its then owned or after-acquired real or personal property, assets, franchises, revenues or income.~~;~~

(11) To construct, maintain, and operate electric transmission and distribution lines along, upon, under and across all public thoroughfares, including without limitation, all roads, highways, streets, alleys, bridges and causeways, and upon, under and across all publicly owned lands, subject, however, to the requirements in respect of the use of such thoroughfares and lands that are imposed by the respective authorities having jurisdiction thereof upon corporations constructing or operating electric transmission and distribution lines or systems.~~;~~

(12) To exercise the power of eminent domain in the manner provided by the laws of this state for the exercise of that power by corporations constructing or operating electric transmission and distribution lines or systems.~~;~~

(13) To provide communications services, as defined in s. 350.81(1), notwithstanding any other provision of law, if the cooperative provides broadband service directly or in partnership with a third party or receives broadband grant funding pursuant to s. 288.9962 or from any other federal or state program offering grants to expand broadband Internet service to unserved areas of this state; however, all poles owned by the cooperative are subject to regulation under s. 366.04(8) on the same basis as if such cooperative were a public utility.

(14) To conduct its business and exercise any or all of



CODING: Words ~~stricken~~ are deletions; words underlined are additions.

its powers within or without this state.~~;~~

(15)~~(14)~~ To adopt, amend, and repeal bylaws.~~; and~~

(16)~~(15)~~ To do and perform any and all other acts and things, and to have and exercise any and all other powers which may be necessary, convenient or appropriate to accomplish the purpose for which the cooperative is organized.

(17) To promote economic development by providing~~, an electric cooperative may provide~~ any energy or nonenergy services to its membership.

Section 2. This act shall take effect July 1, 2023.



CODING: Words ~~stricken~~ are deletions; words underlined are additions.

# HB 1437

# HOUSE OF REPRESENTATIVES STAFF ANALYSIS

**BILL #:** HB 1437 Pub. Rec./Broadband Opportunity Program Information/DEO
**SPONSOR(S):** Esposito
**TIED BILLS:** **IDEN./SIM. BILLS:** CS/SB 552

| REFERENCE | ACTION | ANALYST | STAFF DIRECTOR or BUDGET/POLICY CHIEF |
|---|---|---|---|
| 1) Energy, Communications & Cybersecurity Subcommittee | | Mortellaro | Keating |
| 2) Ethics, Elections & Open Government Subcommittee | | | |
| 3) Commerce Committee | | | |

## SUMMARY ANALYSIS

In 2021, the Legislature created the Broadband Opportunity Program to award grants to applicants who seek to expand access to broadband Internet service in unserved areas of the state. The grant program is administered by the Florida Office of Broadband within the Department of Economic Opportunity (DEO). The grant process requires that certain information about existing and proposed telecommunications facilities be submitted to DEO.

This bill creates a public record exemption for information relating to communications service locations, project proposals, and challenges submitted to and held by DEO under s. 288.9962, F.S. Under the bill, such information is confidential and exempt if it is not otherwise publicly available and would reveal:

- The location and capacity of communications network facilities;
- Communications network coverage areas, including geographical maps;
- Features, functions, and capabilities of communications network infrastructure and facilities;
- Security, including cybersecurity, of the design, construction, and operation of the communications network and associated services and products;
- Specific customer locations; or
- Sources of funding or in-kind contributions for a project.

The bill provides a statement of public necessity for this exemption. The statement provides that disclosing this information could result in identification of vulnerabilities of communications services networks and facilities, thus allowing security breaches that may damage and disrupt the safe and reliable operation of such networks, adversely impacting the public health and safety of the state and affecting business interests through compromised network security.

The bill is subject to the Open Government Sunset Review Act and will repeal on October 2, 2028 unless saved by reenactment.

The bill provides an effective date of July 1, 2023.

**Article I, s. 24(c) of the Florida Constitution requires a two-thirds vote of the members present and voting for final passage of a newly created or expanded public record or public meeting exemption. The bill creates a public record exemption; thus, it requires a two-thirds vote for final passage.**

## FULL ANALYSIS

## I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

**Current Situation**

*Public Record Exemptions*

Article I, section 24(a) of the Florida Constitution establishes the state's public policy for accessing government records. This section guarantees that every person has the right to inspect or copy any public record from the legislative, executive, and judicial branches of government. Authority to grant exemptions from public records is vested solely to the Legislature. The Legislature, may provide an exemption of records, from the requirements of art. I, s. 24(a) of the Florida Constitution.[1] A proposed exemption must pass by a two-thirds vote of each chamber, state with specificity the public necessity to justify the exemption,[2] and be no broader than necessary to accomplish the public purpose.[3]

Public policy regarding access to government records is addressed further in s. 119.07(1), F.S., which guarantees every person a right to inspect and copy any state, county, or municipal record, unless the record is exempt. Public exemptions are subject to the Open Government Sunset Review Act (Act)[4] which provides that a public record or public meeting exemption may be created[5] or maintained only if it serves an identifiable public purpose. In addition, it may be no broader than necessary to meet one of the following purposes:

- Allow the state or its political subdivisions to effectively and efficiently administer a governmental program, which administration would be significantly impaired without the exemption.
- Protect sensitive personal information that, if released, would be defamatory or would jeopardize an individual's safety; however, only the identity of an individual may be exempted under this provision.
- Protect trade or business secrets.[6]

The Act requires the Legislature to review each public record exemption and each public meeting exemption five years after enactment. If the Legislature does not reenact an exemption, it will automatically repeal on October 2nd of the fifth year after enactment.

*Florida's Office of Broadband*

In 2020, the Legislature designated the Department of Economic Opportunity (DEO) as the lead state agency to facilitate the expansion of broadband Internet service in the state.[7] The Florida Office of Broadband (Office) was created within DEO's Division of Community Development for purposes of developing, marketing, and promoting broadband Internet service in the state.[8]

In 2021, the Legislature appropriated $1.5 million to DEO to develop geographic information system maps of broadband Internet service availability, including transmission speeds, consistent with the Federal Communications Commission's data collection program standards.[9] DEO must collaborate with broadband service providers, state agencies, local government entities, private businesses, educational institutions, and community organizations to develop these maps.[10] Through its website, DEO allows

[1] Article I, s. 24(c), FLA. CONST.
[2] This portion of a public record exemption is commonly referred to as a "public necessity statement."
[3] Article I, s. 24(c), FLA. CONST.
[4] S. 119.15, F.S.
[5] An example of an exception to a public record exemption would be allowing another agency access to confidential and exempt records.
[6] S. 119.15(6)(b), F.S.
[7] Ch. 2002-26, Laws of Fla.
[8] *Id.*
[9] Ch. 2021-24, Laws of Fla.
[10] *Id.*

for public input concerning the speed, connectivity, and access to broadband Internet service in areas throughout the state to help identify unserved and underserved areas.

*Broadband Opportunity Program*

In 2021, the Legislature also created the Broadband Opportunity Program[11] to award grants to applicants who seek to expand access to broadband Internet service[12] in unserved[13] areas of the state, regardless of the technology to be used. Grant funds may not be used to provide broadband Internet service to a geographic area where broadband Internet is already deployed by at least one provider.[14] Applicants eligible for grant awards include corporations, limited liability companies, general partnerships, limited partnerships, political subdivisions, and Indian tribes.[15]

In support of a grant application, an applicant must provide specified information, including, among other things:

- A description of the project area;
- A description of the kind and amount of broadband Internet service infrastructure that is proposed; and
- Evidence demonstrating the unserved nature of the project area.[16]

After the close of the grant application process, the Office must publish on its website, from each grant application submitted, the proposed unserved areas to be served and the proposed broadband internet speeds of the areas to be served.[17]

If a broadband Internet service provider provides service in or adjacent to a proposed project area, it can submit a written challenge to the office within 45 days of the information's publication. The challenge must demonstrate:

- The provider currently has deployed broadband Internet service to retail customers within the project area;
- The provider has begun construction to provide broadband Internet service to retail customers within the proposed project area within the timeframe proposed by the applicant; or
- The provider commits to providing broadband Internet service to retail customers within the proposed project area within the timeframe proposed by the applicant.

Within three business days after the submission of a written challenge, the office is to notify the applicant of the challenge. The office must evaluate each challenge submitted. If the office determines that the provider currently has deployed, has begun construction to provide, or commits to provide broadband Internet service in the proposed project area, the office may not fund the challenged project.[18]

[11] Section 288.9962, F.S.
[12] Section 288.9961(2)(a), F.S., defines the term "broadband Internet service" to mean any service that provides access to the Internet with a capacity for transmission at a consistent speed of at least 25 megabits per second download and 3 megabits per second upload.
[13] Section 288.9961(2)(g), F.S., defines the term "unserved" to mean a geographic area of the state without access to broadband Internet service.
[14] S. 288.9962(2), F.S.
[15] S. 288.9962(3), F.S.
[16] S. 288.9962(5), F.S.
[17] S. 288.9962(6)(b), F.S.
[18] S. 288.9962(e), F.S.

**Effect of the Bill**

The bill creates a public record exemption by providing that information relating to communications services locations, project proposals, and challenges submitted to and held by DEO under s. 288.9962, F.S., are confidential and exempt[19] if the information is not otherwise publicly available and would reveal:

- The location and capacity of communications network facilities;
- Communications network coverage areas, including geographical maps indicating actual or proposed locations of network infrastructure, facilities, or coverage;
- Features, functions, and capabilities of communications network infrastructure and facilities;
- Security, including cybersecurity, of the design, construction, and operation of the communications network and associated services and products;
- Specific customer locations;
- Sources of funding or in-kind contributions for a project.

The bill is subject to Open Government Sunset Review Act and shall repeal on October 2, 2028 unless saved through reenactment.

The bill provides that there is a public necessity for this exemption because the information at issue contains security information and propriety business information. The bill states that disclosing locations, capacities, features, and functions of communications networks and facilities could result in identifying vulnerabilities in these networks and facilities which could allow security breaches that may damage and disrupt the safe and reliable operation of such networks and facilities, adversely impacting the public health and safety of the state and affecting business interests through compromising network security.

The bill provides an effective date of July 1, 2023.

B. SECTION DIRECTORY:

**Section 1.** Amends s. 119.0712, F.S., to create a public records exemption for certain information held by the Department of Economic Opportunity.

**Section 2.** Provides a public necessity statement.

**Section 3.** Provides an effective date.

[19] There is a difference between records the Legislature designates exempt from public record requirements and those the Legislature deems confidential and exempt. A record classified as exempt from public disclosure may be disclosed under certain circumstances. See WFTV, Inc. v. Sch. Bd. of Seminole, 874 So.2d 48, 53 (Fla. 5th DCA 2004), review denied 892 So.2d 1015 (Fla. 2004); City of Rivera Beach v. Barfield, 642 So.2d 1135 (Fla. 4th DCA 1994); Williams v. City of Minneola, 575 So.2d 683, 687 (Fla. 5th DCA 1991). If the Legislature designates a record as confidential and exempt from public disclosure, such record may not be released by the custodian of public records, to anyone other than the persons or entities specifically designated in statute. See Op. Att'y Gen. Fla. (1985).

## II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

None.

2. Expenditures:

The bill may have an insignificant negative fiscal impact on DEO. DEO's staff responsible for complying with public record requests may require training related to the newly created public record exemption. These costs, however, would be absorbed, as they are part of the day-to-day responsibilities of the agency.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

None.

2. Expenditures:

None.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

None.

D. FISCAL COMMENTS:

None.

## III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

Not applicable. The bill does not appear to require counties or municipalities to spend funds or take action requiring the expenditure of funds; reduce the authority that counties and municipalities have to raise revenues in the aggregate; or reduce the percentage of state tax shared with counties and municipalities.

2. Other:

Vote Requirement

Article I, section 24(c) of the Florida Constitution requires a two-thirds vote of the members present and voting for final passage of a newly created or expanded public record or public meeting exemption. The bill creates a public record exemption; thus, it requires a two-thirds vote for final passage.

Public Necessity Statement

Article I, section 24(c) of the Florida Constitution requires a public necessity statement for a newly created or expanded public record or public meeting exemption. The bill creates a public record exemption; thus, it includes a public necessity statement.

Breadth of Exemption

Article 1, section 24(c) of the Florida Constitution requires a newly created or expanded public record or public meeting exemption to be no broader than necessary to accomplish the stated purpose of the law. The exemption created by the bill does not appear to be broader than necessary to accomplish its purpose.

B. RULE-MAKING AUTHORITY:

None.

C. DRAFTING ISSUES OR OTHER COMMENTS:

The bill creates a public record exemption for information that reveals communications network coverage areas. This may conflict with the requirement that DEO publish or share certain information related to proposed or existing coverage areas under its broadband grant program.

## IV. AMENDMENTS/COMMITTEE SUBSTITUTE CHANGES

A bill to be entitled

An act relating to public records; amending s. 119.0712, F.S.; providing an exemption from public records requirements for certain information relating to communications services locations, project proposals, and challenges submitted to and held by the Department of Economic Opportunity under the Broadband Opportunity Program; providing for future legislative review and repeal of the exemption; providing a statement of public necessity; providing an effective date.

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

Section 1. Subsection (5) is added to section 119.0712, Florida Statutes, to read:

119.0712 Executive branch agency-specific exemptions from inspection or copying of public records.—

(5) DEPARTMENT OF ECONOMIC OPPORTUNITY.—Information relating to communications services locations, project proposals, and challenges submitted to and held by the Department of Economic Opportunity under s. 288.9962 is confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution if such information is not otherwise publicly available and would reveal:



CODING: Words stricken are deletions; words underlined are additions.

(a) The location and capacity of communications network facilities;

(b) Communications network coverage areas, including geographical maps indicating actual or proposed locations of network infrastructure, facilities, or coverage;

(c) The features, functions, and capabilities of communications network infrastructure and facilities;

(d) Security, including cybersecurity, of the design, construction, and operation of the communications network and associated services and products;

(e) Specific customer locations; or

(f) Sources of funding or in-kind contributions for a project.

This subsection is subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2028, unless reviewed and saved from repeal through reenactment by the Legislature.

Section 2. The Legislature finds that it is a public necessity that information relating to communications services locations, project proposals, and challenges submitted to and held by the Department of Economic Opportunity under s. 288.9962, Florida Statutes, be made exempt from s. 119.07(1), Florida Statutes, and s. 24(a), Article I of the State Constitution if such information is not otherwise publicly

available and would reveal the location and capacity of communications network facilities; communications network coverage areas, including geographical maps indicating actual or proposed locations of network infrastructure, facilities, or coverage; the features, functions, and capabilities of communications network infrastructure and facilities; security, including cybersecurity, of the design, construction, and operation of the communications network and associated services and products; specific customer locations; or sources of funding or in-kind contributions for a project. Such information contains security information and proprietary business information of communications services providers. The disclosure of sensitive information relating to the locations, capacities, features, and functions of communications networks and facilities could result in identification of vulnerabilities in such networks and facilities and allow security breaches that may damage and disrupt the safe and reliable operation of such networks, adversely impacting the public health and safety of the state. Disclosure of such information would adversely affect the business interests and compromise the network security of such communications services providers and their networks and facilities.

Section 3. This act shall take effect July 1, 2023.

# Energy, Communications & Cybersecurity Subcommittee
# HB 1437 by Rep. Esposito
# Pub. Rec./Broadband Opportunity Program Information/DEO

## AMENDMENT SUMMARY
## March 21, 2023

---

**Amendment 1 by Rep. Esposito (lines 22-72):**

- Removes information that reveals communication network coverage areas from the public record exemption created by this bill.
- Clarifies that the exemption does not apply to publication of information by the Department of Economic Opportunity that identifies specified areas proposed to be served, and the broadband Internet speeds in those areas, under the requirements of the state's Broadband Opportunity Program.

COMMITTEE/SUBCOMMITTEE ACTION

| | | |
|---|---|---|
| ADOPTED | ___ | (Y/N) |
| ADOPTED AS AMENDED | ___ | (Y/N) |
| ADOPTED W/O OBJECTION | ___ | (Y/N) |
| FAILED TO ADOPT | ___ | (Y/N) |
| WITHDRAWN | ___ | (Y/N) |
| OTHER | _____ | |

Committee/Subcommittee hearing bill: Energy, Communications & Cybersecurity Subcommittee

Representative Esposito offered the following:

**Amendment**

Remove lines 22-72 and insert:

Department of Economic Opportunity under s. 288.9962 or pursuant to a federal broadband access grant program implemented by the Department of Economic Opportunity is confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution if such information is not otherwise publicly available and the release of such information would reveal:

a. The location or capacity of communications network facilities;

b. Communications network areas, including geographical maps indicating actual or proposed locations of network infrastructure or facilities;

c. The features, functions, and capabilities of communications network infrastructure and facilities;

d. Security, including cybersecurity, of the design, construction, and operation of the communications network and associated services and products;

e. Specific customer locations; or

f. Sources of funding or in-kind contributions for a project.

2. This exemption does not apply to any required functions of the department under s. 288.9962 relating to publishing a description of the proposed unserved areas to be served and the proposed broadband Internet speeds of the areas to be served as provided by the applicant and approved by the department.

3. This paragraph is subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2028, unless reviewed and saved from repeal through reenactment by the Legislature.

Section 2. The Legislature finds that it is a public necessity that certain information relating to communications services locations, project proposals, and challenges submitted to the Department of Economic Opportunity under the Broadband Opportunity Program or pursuant to a federal broadband access

grant program implemented by the department be made confidential and exempt from public records requirements. Such information contains security information and proprietary business information of communications services providers. The disclosure of sensitive information relating to the location, capacity, features, functions, and security of these networks could result in the identification of vulnerabilities in such networks and allow a security breach that could damage the networks or disrupt the networks' safe and reliable operation, adversely impacting the public health and safety of this state. Further, the disclosure of such information would adversely affect the business interests and compromise the network security of the communications services providers and their networks. Therefore, the Legislature finds that it is a public necessity that certain information relating to communications services locations, project proposals, and challenges submitted to the Department of Economic Opportunity under the Broadband Opportunity Program or pursuant to a federal broadband access grant program implemented by the department be held confidential and exempt from disclosure under s. 119.07(1), Florida Statutes, and s. 24(a), Article I of the State Constitution.

# HOUSE OF REPRESENTATIVES STAFF ANALYSIS

**BILL #:** HB 1511 Cybersecurity
**SPONSOR(S):** Giallombardo
**TIED BILLS:** **IDEN./SIM. BILLS:** SB 1708

| REFERENCE | ACTION | ANALYST | STAFF DIRECTOR or BUDGET/POLICY CHIEF |
|---|---|---|---|
| 1) Energy, Communications & Cybersecurity Subcommittee | | Mortellaro | Keating |
| 2) State Administration & Technology Appropriations Subcommittee | | | |
| 3) Commerce Committee | | | |

## SUMMARY ANALYSIS

Over the last decade, cybersecurity has rapidly become a growing concern. Cyberattacks are growing in frequency and severity. Currently, the Department of Management Services (DMS) oversees information technology (IT) governance and security for the executive branch of state government. The Florida Digital Service (FLDS) is housed within DMS and was established in 2020 to replace the Division of State Technology. Through FLDS, DMS implements duties and policies for information technology and cybersecurity for state agencies.

The bill:

- Authorizes FLDS to act more independently from DMS in performing certain functions relating to state technology and cybersecurity, including rulemaking;
- Modifies the definition for "incident";
- Requires FLDS to create an operations committee to foster collaboration between agencies;
- Changes the method by which the state Chief Information Officer (CIO) is appointed;
- Shifts authority to appoint a state chief data officer to the CIO;
- Gives FLDS oversight of the Northwest Regional Data Center (NWRDC);
- Requires FLDS to provide cybersecurity briefings to members of any legislative committee or subcommittee responsible for policy matters relating to cybersecurity;
- Provides that any legislative committee or subcommittee responsible for policy matters relating to cybersecurity may hold meetings closed by the respective legislative body when being briefed on certain information;
- Provides that state agencies shall report a ransomware or cybersecurity incident to FLDS, the Cybersecurity Operations Center, and the Cybercrime Office at FDLE as soon as possible, but no later than four hours after discovery of a cybersecurity incident and no later than two hours after discovery of a ransomware incident;
- Creates a new advisory council called, the State Technology Advancement Council (STAC); and
- Provides grounds for government and private entities to gain a presumption against liability for events connected to a cybersecurity incident.

The bill does not have a fiscal impact on state or local government revenues or local government expenditures. The bill may increase state expenditures. *See* Fiscal Analysis & Economic Impact Statement.

The bill provides an effective date of July 1, 2023.

## FULL ANALYSIS

## I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

**Cybersecurity Governance**

**Present Situation**

Over the last decade, cybersecurity has rapidly become a growing concern. The cyberattacks are growing in frequency and severity. Cybercrime is expected to inflict $8 trillion worth of damage globally in 2023.[1] The United States is often a target of cyberattacks, including attacks on critical infrastructure, and has been a target of more significant cyberattacks[2] over the last 14 years than any other country.[3] The Colonial Pipeline is an example of critical infrastructure that was attacked, disrupting what is arguably the nation's most important fuel conduit.[4]

Ransomware is a type of cybersecurity incident where malware[5] that is designed to encrypt files on a device and renders the files and the systems that rely on them unusable. In other words, critical information is no longer accessible. During a ransomware attack, malicious actors demand a ransom in exchange for regained access through decryption. If the ransom is not paid, the ransomware actors will often threaten to sell or leak the data or authentication information. Even if the ransom is paid, there is no guarantee that the bad actor will follow through with decryption.

In recent years, ransomware incidents have become increasingly prevalent among the nation's state, local, tribal, and territorial government entities and critical infrastructure organizations.[6] For example, Tallahassee Memorial Hospital was hit by a ransomware attack early this February, and the hospitals systems were forced to shut down, impacting many local residents in need of medical care.[7]

*Information Technology and Cybersecurity Management*

The Department of Management Services (DMS) oversees information technology (IT)[8] governance and security for the executive branch in Florida.[9] The Florida Digital Service (FLDS) is housed within DMS and was established in 2020 to replace the Division of State Technology.[10] FLDS works under DMS to implement policies for information technology and cybersecurity for state agencies.[11]

---

[1] Cybercrime Magazine, *Cybercrime to Cost the World $8 Trillion Annually in 2023*, https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/ (last visited March 7, 2023).
[2] "Significant cyber-attacks" are defined as cyber-attacks on a country's government agencies, defense and high-tech companies, or economic crimes with losses equating to more than a million dollars. FRA Conferences, *Study: U.S. Largest Target for Significant Cyber-Attacks*, https://www.fraconferences.com/insights-articles/compliance/study-us-largest-target-for-significant-cyber-attacks/#:~:text=The%20United%20States%20has%20been%20on%20the%20receiving,article%20is%20from%20FRA%27s%20sister%20company%2C%20Compliance%20Week (last visited Mar. 20, 2023).
[3] *Id*.
[4] S&P Global, *Pipeline operators must start reporting cyberattacks to government: TSA orders*, https://www.spglobal.com/commodityinsights/en/market-insights/latest-news/electric-power/052721-pipeline-operators-must-start-reporting-cyberattacks-to-government-tsa-orders?utm_campaign=corporatepro&utm_medium=contentdigest&utm_source=esgmay2021 (last visited Mar. 8, 2023).
[5] "Malware" means hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose. https://csrc.nist.gov/glossary/term/malware (last visited Mar 16, 2023).
[6] Cybersecurity and Infrastructure Agency, *Ransomware 101,* https://www.cisa.gov/stopransomware/ransomware-101 (last visited January 30, 2022).
[7] Tallahassee Democrat, *TMH says it has taken 'major step' toward restoration after cybersecurity incident* (Feb. 15, 2023) https://www.tallahassee.com/story/news/local/2023/02/14/tmh-update-hospital-has-taken-major-step-toward-restoration/69904510007/ (last visited Mar. 7, 2023).
[8] The term "information technology" means equipment, hardware, software, firmware, programs, systems, networks, infrastructure, media, and related material used to automatically, electronically, and wirelessly collect, receive, access, transmit, display, store, record, retrieve, analyze, evaluate, process, classify, manipulate, manage, assimilate, control, communicate, exchange, convert, converge, interface, switch, or disseminate information of any kind or form. S. 282.0041(19), F.S.
[9] *See* s. 20.22, F.S.
[10] Ch. 2020-161, L.O.F.
[11] *See* s. 20.22(2)(b), F.S.

The head of FLDS is appointed by the Secretary of Management Services[12] and serves as the state chief information officer (CIO).[13] The CIO must have at least five years of experience in the development of IT system strategic planning and IT policy and, preferably, have leadership-level experience in the design, development, and deployment of interoperable software and data solutions.[14] FLDS must propose innovative solutions that securely modernize state government, including technology and information services, to achieve value through digital transformation and interoperability, and to fully support Florida's cloud first policy.[15]

DMS, *through* FLDS, has the following powers, duties, and functions:

- Develop IT policy for the management of the state's IT resources;
- Develop an enterprise architecture;
- Establish project management and oversight standards with which state agencies must comply when implementing IT projects;
- Perform project oversight on all state agency IT projects that have a total cost of $10 million or more and that are funded in the General Appropriations Act or any other law; and
- Identify opportunities for standardization and consolidation of IT services that support interoperability, Florida's cloud first policy, and business functions and operations that are common across state agencies.[16]

*Information Technology Security Act*

In 2021, the Legislature passed the IT Security Act,[17] which requires DMS and the state agency[18] heads to meet certain requirements in order to enhance the IT security of the state agencies. Specifically, the IT Security Act provides that DMS is responsible for establishing standards and processes consistent with accepted best practices for IT security,[19] including cybersecurity, and adopting rules that safeguard an agency's data, information, and IT resources to ensure availability, confidentiality, integrity, and to mitigate risks.[20] In addition, DMS must:

- Designate a state chief information security officer (CISO) to oversee state IT security;
- Develop, and annually update, a statewide IT security strategic plan;
- Develop and publish an IT security framework for use by state agencies;
- Collaborate with the Cybercrime Office within the Florida Department of Law Enforcement (FDLE) to provide training; and
- Annually review the strategic and operational IT security plans of executive branch agencies.[21]

*State Cybersecurity Act*

In 2022, the Legislature passed the State Cybersecurity Act,[22] which requires DMS and the heads of the state agencies[23] to meet certain requirements to enhance the cybersecurity[24] of the state agencies.

[12] The Secretary of Management Services serves as the head of DMS and is appointed by the Governor, subject to confirmation by the Senate. S. 20.22(1), F.S.
[13] S. 282.0051(2)(a), F.S.
[14] *Id.*
[15] S. 282.0051(1), F.S.
[16] *Id*.
[17] S. 282.318, F.S.
[18] The term "state agency" means any official, officer, commission, board, authority, council, committee, or department of the executive branch of state government; the Justice Administrative Commission; and the Public Service Commission. The term does not include university boards of trustees or state universities. S. 282.0041(33), F.S. For purposes of the IT Security Act, the term includes the Department of Legal Affairs, The Department of Agriculture and Consumer Services, and the Department of Financial Services. S. 282.318(2), F.S.
[19] The term "information technology security" means the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of data, information, and information technology resources. S. 282.0041(22), F.S.
[20] S. 292.318(3), F.S.
[21] *Id.*
[22] S. 282.318, F.S.
[23] For purposes of the State Cybersecurity Act, the term "state agency" includes the Department of Legal Affairs, the Department of Agriculture and Consumer Services, and the Department of Financial Services. S. 282.318(2), F.S.
[24] "Cybersecurity" means the protection afforded to an automated information system in order to attain the applicable objectives of preserving the confidentiality, integrity, and availability of data, information, and information technology resources. S. 282.0041(8), F.S.

DMS is tasked with completing the following, through FLDS:

- Establishing standards for assessing agency cybersecurity risks;
- Adopting rules to mitigate risk, support a security governance framework, and safeguard agency digital assets, data,[25] information, and IT resources;[26]
- Designating a chief information security officer (CISO);
- Developing and annually updating a statewide cybersecurity strategic plan such as identification and mitigation of risk, protections against threats, and tactical risk detection for cyber incidents;[27]
- Developing and publishing for use by state agencies a cybersecurity governance framework;
- Assisting the state agencies in complying with the State Cybersecurity Act;
- Annually providing training on cybersecurity for managers and team members;
- Annually reviewing the strategic and operational cybersecurity plans of state agencies;
- Tracking the state agencies' implementation of remediation plans;
- Providing cybersecurity training to all state agency technology professionals that develops, assesses, and documents competencies by role and skill level;
- Maintaining a Cybersecurity Operations Center (CSOC) led by the CISO to serve as a clearinghouse for threat information and coordinate with FDLE to support responses to incidents; and
- Leading an Emergency Support Function under the state emergency management plan.[28]

The State Cybersecurity Act requires the head of each state agency to designate an information security manager to administer the state agency's cybersecurity program.[29] The head of the agency has additional tasks in protecting against cybersecurity threats as follows:

- Establish a cybersecurity incident response team with FLDS and the Cybercrime Office, which must immediately report all confirmed or suspected incidents to the CISO;
- Annually submit to DMS the state agency's strategic and operational cybersecurity plans;
- Conduct and update a comprehensive risk assessment to determine the security threats;
- Develop and update written internal policies and procedures for reporting cyber incidents;
- Implement safeguards and risk assessment remediation plans to address identified risks;
- Ensure internal audits and evaluations of the agency's cybersecurity program are conducted;
- Ensure that the cybersecurity requirements for the solicitation, contracts, and service-level agreement of IT and IT resources meet or exceed applicable state and federal laws, regulations, and standards for cybersecurity, including the National Institute of Standards and Technology (NIST)[30] cybersecurity framework;
- Provide cybersecurity training to all agency employees within 30 days of employment; and
- Develop a process that is consistent with the rules and guidelines established by FLDS for detecting, reporting, and responding to threats, breaches, or cybersecurity incidents.[31]

*Florida Cybersecurity Advisory Council*

[25] "Data" means a subset of structured information in a format that allows such information to be electronically retrieved and transmitted. S. 282.0041(9), F.S.
[26] "Information technology resources" means data processing hardware and software and services, communications, supplies, personnel, facility resources, maintenance, and training. S. 282.0041(22), F.S.
[27] "Incident" means a violation or imminent threat of violation, whether such violation is accidental or deliberate, of information technology resources, security, policies, or practices. An imminent threat of violation refers to a situation in which the state agency has a factual basis for believing that a specific incident is about to occur. S. 282.0041(19), F.S.
[28] S. 282.318(3), F.S.
[29] S. 282.318(4)(a), F.S.
[30] NIST, otherwise known as the National Institute of Standards and Technology, "is a non-regulatory government agency that develops technology, metrics, and standards to drive innovation and economic competitiveness at U.S.-based organizations in the science and technology industry." Nate Lord, *What is NIST Compliance*, DataInsider (Dec. 1, 2020), https://www.digitalguardian.com/blog/what-nist-compliance (last visited Mar. 17, 2023).
[31] S. 282.318(4), F.S.

The Florida Cybersecurity Advisory Council[32] (CAC) within DMS[33] assists state agencies in protecting IT resources from cyber threats and incidents.[34] The CAC must assist FLDS in implementing best cybersecurity practices, taking into consideration the final recommendations of the Florida Cybersecurity Task Force – a task force created to review and assess the state's cybersecurity infrastructure, governance, and operations.[35] The CAC meets at least quarterly to:

- Review existing state agency cybersecurity policies;
- Assess ongoing risks to state agency IT;
- Recommend a reporting and information sharing system to notify state agencies of new risks;
- Recommend data breach simulation exercises;
- Assist FLDS in developing cybersecurity best practice recommendations; and
- Examine inconsistencies between state and federal law regarding cybersecurity.[36]

The CAC must work with NIST and other federal agencies, private sector businesses, and private security experts to identify which local infrastructure sectors, not covered by federal law, are at the greatest risk of cyber-attacks and to identify categories of critical infrastructure as critical cyber infrastructure if cyber damage to the infrastructure could result in catastrophic consequences.[37]

The CAC must also prepare and submit a comprehensive report to the Governor, the President of the Senate, and the Speaker of the House of Representatives that includes data, trends, analysis, findings, and recommendations for state and local action regarding ransomware incidents as stated below:

- Descriptive statistics, including the amount of ransom requested, duration of the incident, and overall monetary cost to taxpayers of the incident;
- A detailed statistical analysis of the circumstances that led to the ransomware incident which does not include the name of the state agency or local government, network information, or system identifying information;
- Statistical analysis of the level of cybersecurity employee training and frequency of data backup for the state agencies or local governments that reported incidents;
- Specific issues identified with current policy, procedure, rule, or statute and recommendations to address those issues; and
- Other recommendations to prevent ransomware incidents.

*State Data Center*

In 2022, legislation moved the State Data Center (SDC) from FLDS to DMS, which now operates and maintains the SDC. The SDC provides data center services that comply with applicable state and federal laws, regulations, and policies, including all applicable security, privacy, and auditing requirements.[38] The standards used by the SDC are created through the Information Technology Infrastructure Library (ITIL), the International Organization for Standardization, and the International Electrotechnical Commission (ISO/IEC) 20000, and the Project Management Institute's (PMI) best practices.

*Northwest Regional Data Center*

The Northwest Regional Data Center (NWRDC) is the leading computing provider for educational and governmental communities in Florida. In 2022, NWRDC (located at Florida State University) was declared an official state data center, and the current SDC resources, contracts, and assets were transferred to NWRDC, through contract.[39] This allows for NWRDC to provide services from the SDC

[32] Under Florida law, an "advisory council" means an advisory body created by specific statutory enactment and appointed to function on a continuing basis. Generally, an advisory council is enacted to study the problems arising in a specified functional or program area of state government and to provide recommendations and policy alternatives. S. 20.03(7), F.S.; *See also* s. 20.052, F.S.
[33] S. 282.319(1), F.S.
[34] S. 282.319(2), F.S.
[35] S. 282.319(3), F.S.
[36] S. 282.319(9), F.S.
[37] S. 282.319(10), F.S.
[38] S. 282.201(1), F.S.
[39] S. 282.201(5), F.S.

facility. The NWRDC offers services and 24/7 management support for various IT support solutions, including: public/private cloud services, backup and recovery, storage, managed services, Tallahassee fiber loop, Florida LambdaRail, MyFloridaNet, Florida Power and Light Fibernet, CenturyLink Connectivity, security services, multi-site colocation, and disaster recovery.[40]

*Cyber Incident Response*

The National Cyber Incident Response Plan (NCIRP) was developed according to the direction of Presidential Policy Directive (PPD)-41,[41] by the U.S. Department of Homeland Security. The NCIRP is part of the broader National Preparedness System and establishes the strategic framework for a whole-of-Nation approach to mitigating, responding to, and recovering from cybersecurity incidents posing risk to critical infrastructure.[42] The NCIRP was developed in coordination with federal, state, local, and private sector entities and is designed to interface with industry best practice standards for cybersecurity, including the NIST Cybersecurity Framework.

The NCIRP adopted a common schema for describing the severity of cybersecurity incidents affecting the U.S. The schema establishes a common framework to evaluate and assess cybersecurity incidents to ensure that all departments and agencies have a common view of the severity of a given incident; urgency required for responding to a given incident; seniority level necessary for coordinating response efforts; and level of investment required for response efforts.[43]

The severity level of a cybersecurity incident in accordance with the NCIRP is determined as follows:

- Level 5: An emergency-level incident within the specified jurisdiction if the incident poses an imminent threat to the provision of wide-scale critical infrastructure services; national, state, or local security; or the lives of the country's, state's, or local government's citizens.
- Level 4: A severe-level incident if the incident is likely to result in a significant impact within the affected jurisdiction which affects the public health or safety; national, state, or local security; economic security; or individual civil liberties.
- Level 3: A high-level incident if the incident is likely to result in a demonstrable impact in the affected jurisdiction to public health or safety; national, state, or local security; economic security; civil liberties; or public confidence.
- Level 2: A medium-level incident if the incident may impact public health or safety; national, state, or local security; economic security; civil liberties; or public confidence.
- Level 1: A low-level incident if the incident is unlikely to impact public health or safety; national, state, or local security; economic security; or public confidence.[44]

State agencies and local governments in Florida, must report all ransomware incidents and any cybersecurity incidents at severity levels three, four, and five incident as soon as possible, but no later than 48 hours after discovery of a cybersecurity incident and no later than 12 hours after discovery of a ransomware incident, to the Cybersecurity Operations Center (CSOC).[45] The CSOC shall notify the President of the Senate and the Speaker of the House of Representatives of any severity level three, four, or five as soon as possible, but no later than 12 hours after receiving the incident report from the state agency or local government.[46] For state agency incidents at severity levels one and two, they must report these to the CSOC and the Cybercrime Office at FDLE as soon as possible.[47]

[40] NWRDC: Florida's Cloud Broker, *About Northwest Regional Data Center*, at https://www.nwrdc.fsu.edu/about (last visited Mar. 15, 2023).
[41] Annex for PPD-41: *U.S. Cyber Incident Coordination*, available at: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/annex-presidential-policy-directive-united-states-cyber-incident (last visited Mar. 15, 2023).
[42] Cybersecurity & Infrastructure Security Agency, *Cybersecurity Incident Response*, available at https://www.cisa.gov/topics/cybersecurity-best-practices/organizations-and-cyber-safety/cybersecurity-incident-response#:~:text=%20National%20Cyber%20Incident%20Response%20Plan%20%28NCIRP%29%20The,incidents%20and%20how%20those%20activities%20all%20fit%20together (last visited Mar. 15, 2023).
[43] *Id.*
[44] S. 282.318(3)(c)9.a, F.S.
[45] S. 282.318(3)(c)9.c, F.S.
[46] S. 282.318(3)(c)9.c.(II), F.S.
[47] S. 282.318(3)(c)(9)(d), F.S.

The notification must include a high-level description of the incident and the likely effects. An incident report for a cybersecurity or ransomware incident by a state agency or local government must include, at a minimum:

- A summary of the facts surrounding the cybersecurity or ransomware incident;
- The date on which the state agency or local government most recently backed up its data, the physical location of the backup, if the backup was affected, and if the backup was created using cloud computing;
- The types of data compromised by the cybersecurity or ransomware incident;
- The estimated fiscal impact of the cybersecurity or ransomware incident;
- In the case of a ransomware incident, the details of the ransom demanded; and
- If the reporting entity is a local government, a statement requesting or declining assistance from the CSOC, FDLE Cybercrime Office, or sheriff.[48]

In addition, the CSOC must provide consolidated incident reports to the President of the Senate, Speaker of the House of Representatives, and the CAC on a quarterly basis.[49] The consolidated incident reports to the CAC may not contain any state agency or local government name, network information, or system identifying information, but must contain sufficient relevant information to allow the CAC to fulfill its responsibilities.[50]

Legislation passed in 2022 additionally requires state agencies and local governments to submit an after-action report to FLDS within one week of the remediation of a cybersecurity or ransomware incident.[51] The report must summarize the incident, state the resolution, and any insights from the incident.

**Effect of the Bill**

The bill creates the "Florida Cyber Protection Act."

The bill shifts authorities related to cybersecurity governance that the Department of Management Services (DMS) has under current law to the FLDS. In doing so, the bill allows FLDS to make decisions and have oversight, without having to act through DMS. The bill explicitly gives FLDS the authority to respond to any state agency cybersecurity incident.

The bill modifies the definition for "incident" to include anything that may "jeopardize the confidentiality, integrity, or availability of an information technology system or the information the system processes, stores, or transmits." The definition of "ransomware" is amended to include incidents commonly referred to as "cyberextortion."

Under the bill, FLDS must create an operations committee. The committee is formed to develop collaborative efforts between agencies on cybersecurity issues. The CIO is to serve as the executive director of the committee which will be composed of:

- The Attorney General, or his or her designee;
- The Secretary of State, or his or her designee;
- The Executive director of the Department of Law Enforcement, or his or her designee;
- A representative from each state agency;
- A representative of the Florida State Guard; and
- A representative of the Florida National Guard.

The bill changes the method by which the CIO is appointed, requiring the Governor to appoint the position subject to confirmation by the Senate. The bill removes the requirement that the CIO consult the Secretary of Management Services when appointing a state chief data officer.

[48] S. 282.318(3)(c)9.b, F.S.
[49] S. 282.318(3)(c)9.e, F.S.
[50] *Id*.
[51] S. 282.318(4)(k), F.S.

The bill reduces the cost threshold at which state agencies must report information technology projects to FLDS. Under the bill, state agencies must report such projects if the cost is $5 million or more.

The bill shifts oversight of the state data center to FLDS, and with this shift, FLDS will receive full access to the state data center infrastructure. All of DMS's responsibilities with the data center shift to FLDS, including appointing a director of the state data center.

The bill also gives FLDS oversight for the Northwest Regional Data Center (NWRDC). Accordingly, NWRDC is to provide FLDS with access to information regarding operations of the state data center.

Under the bill, FLDS must oversee any cybersecurity audit completed by a private sector vendor to ensure it meets applicable standards, processes, and timelines.

The bill provides that state agencies shall report a ransomware or cybersecurity incident to FLDS, the CSOC, and the Cybercrime Office at FDLE as soon as possible, but no later than four hours after discovery of a cybersecurity incident and no later than two hours after discovery of a ransomware incident. Furthermore, the bill requires FLDS to notify the Governor, President of the Senate, and the Speaker of the House of any incident discovered by a state agency but not timely reported. The reporting requirement is for all severity levels of cyber incidents.

The bill requires that when the CSOC notifies the President of the Senate and the Speaker of the House of Representatives of any level 3, 4, or 5 incident, the notification must be provided in a secure environment. The bill removes the requirement under current law that a state agency must report an incident determined to be of severity levels 1 or 2 to the CSOC and the Cybercrime Office at FDLE.

The bill requires FLDS to provide cybersecurity briefings to members of any legislative committee or subcommittee responsible for policy matters relating to cybersecurity. Any legislative committee or subcommittee responsible for policy matters relating to cybersecurity may hold meetings closed by the respective legislative body at which the committee or subcommittee is briefed on records which are to be made confidential and exempt.

The bill makes the state CIO a member of the Florida Cybersecurity Advisory Council (CAC), replacing the Secretary of Management Services. Members of any legislative committee or subcommittee responsible for policy matters relating to cybersecurity must be invited to and may attend meetings of the CAC. The bill provides that a meeting of the CAC at which two or more members of the Legislature are in attendance may not be construed as a meeting of a legislative committee or subcommittee or as a prearranged gathering between more than two members of the legislature where they are meeting to agree on a formal legislative action.

The bill creates a new advisory council called the State Technology Advancement Council (STAC). STAC is created within the Executive Office of the Governor. The bill states that the purpose of STAC is to:

- Assist state agencies and advise the legislature on innovative technologies;
- Improve state technology project timelines;
- Develop efficient state technology processes;
- Assist in creation of development and testing environments that allow state entities to proof technology concepts before engaging in procurement and otherwise developing processes to reduce wasteful spending on inappropriate technology;
- Assist the Florida College System institutions and state universities with technology transfer processes; and
- Support research on and development of innovative technologies.

Under the bill, the state CIO, or his or her designee, shall serve as the executive director of STAC. STAC is to be comprised of the following members appointed by the Governor:

- A person with senior level experience in cloud computing technology;
- An engineer;
- A person with senior level experience in the space industry;

- A data scientist; and
- Other persons with relevant experience as determined by the Governor.

The bill requires that members serve terms of four years except the first year. For the purposes of providing staggered terms, the initial appointments of two of the members appointed shall be for two years instead of four. All members of the council are eligible for reappointment. The state CIO shall serve as a non-voting member. Members shall serve without compensation but are entitled to receive reimbursement for per diem and travel expenses. The bill requires that members of STAC maintain the confidential or exempt status of information received in the performance of their duties and responsibilities as members of the STAC. The council shall meet at least quarterly.

Beginning June 1, 2024, and annually on June 1 after STAC is created, the STAC must submit a report describing its activities and recommendations to the Governor, Senate President, and Speaker of the House of Representatives.

The bill requires that invoices must be sent to FLDS rather than DMS under s.1004.649, F.S.

**Presumption Against Liability**

**Present Situation**

*Access to Courts*

The Florida Constitution broadly protects the right to access the courts, which "shall be open to every person for redress of any injury..."[52] However, this constitutional right is not unlimited.

In *Kluger v. White*,[53] the Court stated that it would not completely prohibit the Legislature from altering a cause of action, but neither would it allow the Legislature "to destroy a traditional and long-standing cause of action upon mere legislative whim..." The takeaway from *Kluger* and other relevant case law is that the Legislature may:

- Reduce the right to bring a cause of action as long as the right is not entirely abolished.[54]
- Abolish a cause of action that is not "traditional and long-standing"—that is, a cause of action that did not exist at common law, and that did not exist in statute before the adoption of the Florida Constitution's Declaration of Rights.[55]
- Abolish a cause of action if the Legislature either:
  - Provides a reasonable commensurate benefit in exchange;[56] or
  - Shows an "overpowering public necessity for the abolishment of such right, and no alternative method of meeting such public necessity can be shown."[57]

*Tort Liability and Negligence*

[52] Art. I, s. 21, Fla. Const.
[53] *Kluger*, 281 So. 2d 1.
[54] *See Achord v. Osceola Farms Co.*, 52 So. 3d 699 (Fla. 2010).
[55] *See Anderson v. Gannett Comp.*, 994 So. 2d 1048 (Fla. 2008) (false light was not actionable under the common law); *McPhail v. Jenkins*, 382 So. 2d 1329 (Fla. 1980) (wrongful death was not actionable under the common law); *see also Kluger*, 281 So. 2d at 4 ("We hold, therefore, that where a right of access to the courts for redress for a particular injury has been provided by statutory law predating the adoption of the Declaration of Rights of the Constitution of the State of Florida, or where such right has become a part of the common law of the State . . . the Legislature is without power to abolish such a right without providing a reasonable alternative . . . unless the Legislature can show an overpowering public necessity. . .").
[56] *Kluger*, 281 So. 2d at 4; *see Univ. of Miami v. Echarte*, 618 So. 2d 189 (Fla. 1993) (upholding a statutory cap on medical malpractice damages because the Legislature provided arbitration, which is a "commensurate benefit" for a claimant); *accord Lasky v. State Farm Ins. Co.*, 296 So. 2d 9 (Fla. 1974); *but see Smith v. Dept. of Ins.*, 507 So. 2d 1080 (Fla. 1992) (striking down a noneconomic cap on damages, which, while not wholly abolishing a cause of action, did not provide a commensurate benefit).
[57] *Kluger*, 281 So. 2d at 4-5 (noting that in 1945, the Legislature abolished the right to sue for several causes of action, but successfully demonstrated "the public necessity required for the total abolition of a right to sue") (citing *Rotwein v. Gersten*, 36 So. 2d 419 (Fla. 1948); *see Echarte*, 618 So. 2d at 195 ("Even if the medical malpractice arbitration statutes at issue did not provide a commensurate benefit, we would find that the statutes satisfy the second prong of *Kluger* which requires a legislative finding that an 'overpowering public necessity' exists, and further that 'no alternative method of meeting such public necessity can be shown'").

A "tort" is a wrong for which the law provides a remedy. The purpose of tort law is to fairly compensate a person harmed by another person's wrongful acts, whether intentional, reckless, or negligent, through a civil action or other comparable process. A properly-functioning tort system:

- Provides a fair and equitable forum to resolve disputes;
- Appropriately compensates legitimately harmed persons;
- Shifts the loss to responsible parties;
- Provides an incentive to prevent future harm; and
- Deters undesirable behavior.[58]

"Negligence" is a legal term for a type of tort action that is unintentionally committed. In a negligence action, the plaintiff is the party that brings the lawsuit, and the defendant is the party that defends against it. To prevail in a negligence lawsuit, a plaintiff must demonstrate that the:

- Defendant had a legal duty of care requiring the defendant to conform to a certain standard of conduct for the protection of others, including the plaintiff, against unreasonable risks;
- Defendant breached his or her duty of care by failing to conform to the required standard;
- Defendant's breach caused the plaintiff's injury; and
- Plaintiff suffered actual damage or loss resulting from his or her injury.[59]

Courts distinguish varying degrees of civil negligence by using terms such as:

| | |
|---|---|
| **Slight Negligence** | The failure to exercise great care. This often applies to injuries caused by common carries charged with the duty to exercise the highest degree of care toward their passengers.[60] |
| **Ordinary Negligence** | The failure to exercise that degree of care which an ordinary prudent person would exercise; or, in other words, a course of conduct which a reasonable and prudent person would know might possibly result in injury to others.[61] |
| **Gross Negligence** | A course of conduct which a reasonable and prudent person knows would probably and most likely result in injury to another.[62] To prove gross negligence, a plaintiff must usually show that the defendant had knowledge or awareness of imminent danger to another and acted or failed to act with a conscious disregard for the consequences.[63] Once proven, gross negligence may support a punitive[64] damages award.[65] |

In Florida, before a court awards damages in a negligence action, the jury generally assigns a fault percentage to each party under the comparative negligence rule. Florida applies[66] a "pure" comparative negligence rule, which allows a plaintiff to recover damages proportional to his or her fault percentage.[67] For example, if a plaintiff is 40 percent at fault for an accident causing the plaintiff's injury and the defendant is 60 percent at fault, the plaintiff would recover 60 percent of his or her damages.

The Florida Rules of Civil Procedure generally require a plaintiff in a civil action to file a complaint, and require a defendant to file an answer to the complaint.[68] Florida is a "fact-pleading jurisdiction." This

[58] Am. Jur. 2d Torts s. 2.
[59] 6 *Florida Practice Series* s. 1.1; *see Barnett v. Dept. of Financial Services*, 303 So. 3d 508 (Fla. 2020).
[60] *See Faircloth v. Hill*, 85 So. 2d 870 (Fla. 1956); *see also Holland America Cruises, Inc. v. Underwood*, 470 So. 2d 19 (Fla. 2d DCA 1985); *Werndli v. Greyhound Corp.*, 365 So. 2d 177 (Fla. 2d DCA 1978); 6 *Florida Practice Series* s. 1.2.
[61] *See De Wald v. Quarnstrom*, 60 So. 2d 919 (Fla. 1952); *see also Clements v. Deeb*, 88 So. 2d 505 (Fla. 1956); 6 *Florida Practice Series* s. 1.2.
[62] *See Clements*, 88 So. 2d 505; 6 *Florida Practice Series* s. 1.2.
[63] *See Carraway v. Revell*, 116 So. 2d 16 (Fla. 1959).
[64] Punitive damages are awarded in addition to actual damages to punish a defendant for behavior considered especially harmful. Florida generally caps punitive damage awards at $500,000 or triple the value of compensatory damages, whichever is greater, and caps cases of intentional misconduct with a financial motivation at two million dollars or four times the amount of compensatory damages, whichever is greater. S. 768.73(1), F.S.
[65] *See Glaab v. Caudill*, 236 So. 2d 180 (Fla. 2d DCA 1970); 6 *Florida Practice Series* s. 1.2; s. 768.72(2), F.S.
[66] The comparative negligence standard does not apply to any action brought to recover economic damages from pollution, based on an intentional tort, or to which the joint and several liability doctrines is specifically applied in chs. 403, 498, 517, 542, and 895, F.S. S. 768.81(4), F.S.
[67] S. 768.81(2), F.S.; *see Williams v. Davis*, 974 So. 2d 1052 (Fla. 2007).
[68] Fla. R. Civ. P. 1.100.

means that a pleading setting forth a claim for relief, including a complaint, must generally state a cause of action and contain a:

- Short and plain statement of the grounds on which the court's jurisdiction depends, unless the court already has jurisdiction and the claim needs no new grounds to support it;
- Short and plain statement of the ultimate facts[69] showing the pleader is entitled to relief; and
- Demand for the relief to which the pleader believes he or she is entitled to.[70]

However, certain allegations[71] must be plead with "particularity," which is a heightened level of pleading requiring a statement of facts sufficient to satisfy the elements of each claim.

*Burden of Proof and Presumptions*

The burden of proof is an obligation to prove a material fact in issue.[72] Generally, the party who asserts the material fact in issue has the burden of proof.[73] In a civil proceeding, for example, the burden of proof is on the plaintiff to prove the allegations contained in his or her complaint. Further, a defendant in either a criminal or a civil proceeding has the burden to prove any affirmative defenses[74] he or she may raise in response to the charges or allegations. However, there are certain statutory and common law presumptions[75] that may shift the burden of proof from the party asserting the material fact in issue to the party defending against such fact.[76] These presumptions remain in effect following the introduction of evidence rebutting the presumption, and the factfinder must decide if such evidence is strong enough to overcome the presumption.[77] A presumption is a legal inference that can be made with knowing certain facts. Most presumptions are able to be rebutted, if proven to be false or thrown into sufficient doubt by the evidence.[78]

*Cybersecurity Standards*

Per Florida law, local governments are required to adopt cybersecurity standards that safeguard the local government's data, information technology, and information technology resources to ensure availability, confidentiality, and integrity.[79] The standards must be consistent with generally accepted best practices for cybersecurity, including the NIST cybersecurity framework.[80] Once the standards are adopted, each local government is to notify FLDS as soon as possible.[81]

The National Institute for Standards and Technology (NIST) is a non-regulatory federal agency housed within the U.S. Department of Commerce. NIST is charged with providing a prioritized, flexible, repeatable, performance-based, and cost-effective framework that helps owners and operators of critical infrastructure identify, assess, and manage cyber risk. While the framework was developed with critical infrastructure in mind, it can be used by organizations in any sector of the economy or society.[82] The framework is designed to complement, and not replace, an organization's own unique approach to cybersecurity risk management. As such, there are a variety of ways to use the framework and the

[69] Ultimate facts are facts that must be accepted for a claim to prevail, usually inferred from a number of supporting evidentiary facts, which themselves are facts making other facts more probable. *See* Legal Information Institute, *Ultimate Fact*, https://www.law.cornell.edu/wex/ultimate_fact (last visited Mar. 16, 2023); *see also* Legal Information Institute, *Evidentiary Facts*, https://www.law.cornell.edu/wex/evidentiary_fact (last visited Mar. 16, 2023).
[70] *See Goldschmidt v. Holman*, 571 So. 2d 422 (Fla. 1990); Fla. R. Civ. P. 1.110.
[71] These allegations include fraud, mistake, condition of the mind, and denial of performance or occurrence. Fla. R. Civ. P. 1.120(b),(c).
[72] 5 *Florida Practice Series* s. 16:1.
[73] *Id.*; *see Berg v. Bridle Path Homeowners Ass'n, Inc.*, 809 So. 2d 32 (Fla. 4th DCA 2002).
[74] An affirmative defense is a defense which, if proven, negates criminal or civil liability even if it is proven that the defendant committed the acts alleged. Examples include self-defense, entrapment, insanity, necessity, and *respondeat superior*. Legal Information Institute, *Affirmative Defense*, https://www.law.cornell.edu/wex/affirmative_defense (last visited Mar. 16, 2021).
[75] These presumptions tend to be social policy expressions, such as the presumption that all people are sane or that all children born in wedlock are legitimate. 5 *Florida Practice Series* s. 16:1.
[76] 5 *Florida Practice Series* s. 16:1.
[77] *Id.*
[78] Legal Information Institute, *Presumption*, https://www.law.cornell.edu/wex/presumption (last visited Mar. 16, 2023).
[79] S.282.3185(4)(a), F.S.
[80] *Id.*
[81] S.282.3185(4)(d), F.S.
[82] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (last visited March 7, 2023).

decision about how to apply it is left to the implementing organization. For example, an organization may use its current processes and consider the framework to identify opportunities to strengthen its cybersecurity risk management. The framework, overall, provides an outline of best practices that helps organizations decide where to focus resources for cybersecurity protection.[83] Other cybersecurity standards include:

| | |
|---|---|
| **NIST special publication 800-171** | Provides recommended requirements for protecting the confidentiality of controlled unclassified information. If a manufacturer is part of a Department of Defense, General Services Administration, NASA, or other state or federal agency supply chain then they must comply with these security requirements.[84] |
| **NIST special publications 800-53 and 800-53A** | A category of security and privacy controls. Covers the steps in the Risk Management Framework that address security controls for federal information systems.[85] |
| **The Federal Risk and Authorization Management Program security assessment framework** | Organization established by the General Services Administration (a Federal Government Program) that provides U.S. federal agencies, state agencies, and their vendors with a standardized set of best practices to assess, adopt, and monitor the use of cloud-based technology services under the Federal Information Security Management Act (FISMA).[86] |
| **CIS Critical Security Controls** | The Center for Internet Security Critical Security Controls (CIS) are a prescriptive and simplified set of best practices for strengthening cybersecurity for different organizations. CIS was created in response to extreme data losses experienced by organizations in the U.S. defense industrial base.[87] |
| **The International Organization for Standardization/International Electrotechnical Commission 27000 – series family of standards** | ISO/IEC 27001 (ISO) enables organizations of all sectors to manage security of financial information, intellectual property, employee data and information entrusted by third parties. ISO has auditors and is an international standard. There are 804 technical committees and subcommittees concerned with such standards of development.[88] |

**Effect of the Bill**

The bill provides a presumption against liability for events connected to a cybersecurity incident. Under the bill:

- A county or municipality that substantially complies with s. 282.3185, F.S., shall gain a presumption against liability.

[83] *Id.*
[84] NIST, *What is the NIST SP 800-171 and Who Needs to Follow It?*, https://www.nist.gov/blogs/manufacturing-innovation-blog/what-nist-sp-800-171-and-who-needs-follow-it-0#:~:text=NIST%20SP%20800-171%20is%20a%20NIST%20Special%20Publication,protecting%20the%20confidentiality%20of%20controlled%20unclassified%20information%20%28CUI%29 (last visited Mar. 15, 2023).
[85] NIST, *Selecting Security and Privacy Controls: Choosing the Right Approach*, https://www.nist.gov/blogs/cybersecurity-insights/selecting-security-and-privacy-controls-choosing-right-approach (last visited Mar. 16, 2023).
[86] Reciprocity, *How State and Local Agencies Can Use FedRAMP*, https://reciprocity.com/how-state-and-local-agencies-can-use-fedramp/#:~:text=The%20Federal%20Risk%20and%20Authorization%20Management%20Program%20%28FedRAMP%29,cloud%20products%20offered%20by%20cloud%20service%20providers%20%28CSPs%29 (last visited Mar. 16, 2023).
[87] CIS Security, *CIS Critical Security Controls*, https://www.cisecurity.org/controls (last visited Mar. 16, 2023).
[88] ITGovernance, *ISO 27001, The International Security Standard*, https://www.itgovernanceusa.com/iso27001#:~:text=ISO%2027001%20is%20a%20globally%20recognized%20information%20security,trusted%20benchmark.%20Protect%20your%20data%2C%20wherever%20it%20lives (last visited Mar. 16, 2023).

- A sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity acquires, maintains, stores, or uses personal information shall gain a presumption against liability if the entity substantially complies with s. 501.171, F.S., and has adopted a cybersecurity program that substantially aligns with the current version of any of the following:
    - National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity.
    - NIST special publication 800-171.
    - NIST special publications 800-53 and 800-53A.
    - The Federal Risk and Authorization Management Program security assessment framework.
    - CIS Critical Security Controls
    - The International Organization for Standardization/International Electrotechnical Commission 27000 – series family of standards; or
    - If the entity is regulated by the state or Federal Government, or both, or if otherwise subject to the requirements of any of the following laws and regulations, it must substantially comply its cybersecurity program to the current version of:
        - The security requirements of the Health Insurance Portability and Accountability Act of 1996;
        - Title V of the Gramm-Leach-Bliley Act of 1999 as amended;
        - The Federal Information Security Modernization Act of 2014; or
        - The Health Information Technology for Economic and Clinical Health Act.

A commercial entity that substantially complies with a combination of industry-recognized cybersecurity frameworks or standards, including the payment card industry data security standard, gains a presumption against liability, and must adopt the revised frameworks or standards within 1 year after the latest publication date stated in the revisions.

The bill does not establish a private cause of action. It provides that a failure of a county, municipality, or commercial entity to substantially implement a cybersecurity program that would allow it to gain a presumption against liability under the bill is not evidence of negligence and does not constitute negligence per se.

The bill provides that the act shall take effect July 1, 2023

B. SECTION DIRECTORY:

**Section 1:** Provides a short title for the act.

**Section 2:** Amends s. 282.0041, F.S., relating to definitions.

**Section 3:** Amends s. 282.0051, F.S. relating to DMS; FLDS; powers, duties, and functions.

**Section 4:** Amends s. 282.201, F.S., relating to the State Data Center.

**Section 5:** Amends s. 282.318, F.S., relating to cybersecurity.

**Section 6:** Amends s. 282.3185, F.S., relating to local government cybersecurity.

**Section 7:** Amends and adds to s. 282.319, F.S., relating to Florida Cybersecurity Advisory Council.

**Section 8:** Creates s. 282.3195, F.S., creating a State Technology Advancement Council.

**Section 9:** Creates s. 768.401, F.S., creating a presumption against liability.

**Section 10:** Amends s. 1004.649, F.S., relating to the Northwest Regional Data Center.

**Section 11:** Provides an effective date of July 1, 2023.

## II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

   None.

2. Expenditures:

   The bill may impose additional expenditures on FLDS, as many oversight tasks shift to FLDS. Additionally, the per diem expenses of the newly created State Technology Advancement Council may result in increased expenditures.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

   None.

2. Expenditures:

   None.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

None.

D. FISCAL COMMENTS:

None.

## III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

   Not applicable. This bill does not appear to require counties or municipalities to spend funds or take action requiring the expenditures of funds; reduce the authority that counties or municipalities have to raise revenues in the aggregate; or reduce the percentage of state tax shared with counties or municipalities.

2. Other:

   None.

B. RULE-MAKING AUTHORITY:

The bill shifts the authority to adopt rules relating to cybersecurity and the administration of s. 282.318, F.S., from DMS to FLDS.

C. DRAFTING ISSUES OR OTHER COMMENTS:

None.

## IV. AMENDMENTS/COMMITTEE SUBSTITUTE CHANGES

A bill to be entitled

An act relating to cybersecurity; providing a short title; amending s. 282.0041, F.S.; revising definitions; amending s. 282.0051, F.S.; clarifying the powers, duties, and functions of the Florida Digital Service; revising the cost threshold of state agency information technology projects for which the Florida Digital Service must perform project oversight; requiring the Florida Digital Service to establish an operations committee for a certain purpose and composed of certain members; requiring the Governor to appoint a state chief information officer subject to confirmation by the Senate; conforming provisions to changes made by the act; amending s. 282.201, F.S.; requiring the Florida Digital Service to oversee the state data center; requiring the Florida Digital Service to be provided with full access to state data center infrastructure; requiring the Northwest Regional Data Center to provide the Florida Digital Service with access to certain information; conforming provisions to changes made by the act; amending s. 282.318, F.S.; clarifying the authority of the Florida Digital Service; requiring the Florida Digital Service to oversee certain cybersecurity audits; requiring a state agency to

report ransomware and cybersecurity incidents within a certain time period; requiring the Florida Digital Service to notify the Governor and Legislature of certain incidents; providing that certain notification must be provided in a secure environment; requiring the Florida Digital Service to provide cybersecurity briefings to certain legislative committees; authorizing the Florida Digital Service to respond to certain cybersecurity incidents; authorizing certain legislative committees to hold closed meetings to receive certain briefings; requiring such committees to maintain the confidential and exempt status of certain records; amending s. 282.3185, F.S.; requiring a local government to report ransomware and cybersecurity incidents within a certain time period; requiring the Florida Digital Service to notify the Governor and Legislature of certain incidents; providing that certain notification must be provided in a secure environment; amending s. 282.319, F.S.; revising the membership of the Florida Cybersecurity Advisory Council; providing that members of certain legislative committees must be invited to and may attend meetings of the council; providing construction; creating s. 282.3195, F.S.; creating the State Technology Advancement Council within the

Executive Office of the Governor; providing for the purpose, membership, terms of office, and meetings of the council and members; providing requirements for members relating to confidential and exempt information and certain agreements; requiring the council to submit an annual report to the Governor and Legislature beginning on a specified date; creating s. 768.401, F.S.; providing a presumption against liability in connection with a cybersecurity incident for a county, municipality, or commercial entity that complies with certain requirements; requiring certain entities to adopt certain revised frameworks or standards within a specified time period; providing that a private cause of action is not established; providing that certain failures are not evidence of negligence and do not constitute negligence per se; amending s. 1004.649, F.S.; conforming provisions to changes made by the act; providing an effective date.

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

Section 1. This act may be cited as the "Florida Cyber Protection Act."

Section 2. Subsections (1), (7), (19), and (28) of section 282.0041, Florida Statutes, are amended to read:

282.0041 Definitions.—As used in this chapter, the term:

(1) "Agency assessment" means the amount each customer entity must pay annually for services from the Florida Digital Service ~~Department of Management Services~~ and includes administrative and data center services costs.

(7) "Customer entity" means an entity that obtains services from the Florida Digital Service ~~Department of Management Services~~.

(19) "Incident" means a violation or an imminent threat of violation, whether such violation is accidental or deliberate, of information technology resources, security, policies, or practices which may jeopardize the confidentiality, integrity, or availability of an information technology system or the information the system processes, stores, or transmits. An imminent threat of violation refers to a situation in which a state agency, county, or municipality has a factual basis for believing that a specific incident is about to occur.

(28) "Ransomware incident" means a malicious cybersecurity incident in which a person or an entity introduces software that gains unauthorized access to or encrypts, modifies, or otherwise renders unavailable a state agency's, county's, or municipality's data and thereafter the person or entity demands a ransom to prevent the publication of the data, restore access to the data, or otherwise remediate the impact of the software. Such incidents are commonly referred to as cyberextortion.

Section 3. Section 282.0051, Florida Statutes, is amended to read:

282.0051 Department of Management Services; Florida Digital Service; powers, duties, and functions.—

(1) The Florida Digital Service is ~~has been~~ created within the department to propose innovative solutions that securely modernize state government, including technology and information services, to achieve value through digital transformation and interoperability, and to fully support the cloud-first policy as specified in s. 282.206. The ~~department, through the~~ Florida Digital Service~~,~~ shall have the following powers, duties, and functions:

(a) Develop and publish information technology policy for the management of the state's information technology resources.

(b) Develop an enterprise architecture that:

1. Acknowledges the unique needs of the entities within the enterprise in the development and publication of standards and terminologies to facilitate digital interoperability;

2. Supports the cloud-first policy as specified in s. 282.206; and

3. Addresses how information technology infrastructure may be modernized to achieve cloud-first objectives.

(c) Establish project management and oversight standards with which state agencies must comply when implementing information technology projects. The ~~department, acting through~~

~~the~~ Florida Digital Service~~,~~ shall provide training opportunities to state agencies to assist in the adoption of the project management and oversight standards. To support data-driven decisionmaking, the standards must include, but are not limited to:

1. Performance measurements and metrics that objectively reflect the status of an information technology project based on a defined and documented project scope, cost, and schedule.

2. Methodologies for calculating acceptable variances in the projected versus actual scope, schedule, or cost of an information technology project.

3. Reporting requirements, including requirements designed to alert all defined stakeholders that an information technology project has exceeded acceptable variances defined and documented in a project plan.

4. Content, format, and frequency of project updates.

5. Technical standards to ensure an information technology project complies with the enterprise architecture.

(d) Perform project oversight on all state agency information technology projects that have total project costs of $5 ~~$10~~ million or more and that are funded in the General Appropriations Act or any other law. The ~~department, acting through the~~ Florida Digital Service~~,~~ shall report at least quarterly to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives

on any information technology project that the Florida Digital Service ~~department~~ identifies as high-risk due to the project exceeding acceptable variance ranges defined and documented in a project plan. The report must include a risk assessment, including fiscal risks, associated with proceeding to the next stage of the project, and a recommendation for corrective actions required, including suspension or termination of the project.

(e) Identify opportunities for standardization and consolidation of information technology services that support interoperability and the cloud-first policy, as specified in s. 282.206, and business functions and operations, including administrative functions such as purchasing, accounting and reporting, cash management, and personnel, and that are common across state agencies. The ~~department, acting through the~~ Florida Digital Service~~,~~ shall biennially on January 1 of each even-numbered year provide recommendations for standardization and consolidation to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives.

(f) Establish best practices for the procurement of information technology products and cloud-computing services in order to reduce costs, increase the quality of data center services, or improve government services.

(g) Develop standards for information technology reports

and updates, including, but not limited to, operational work plans, project spend plans, and project status reports, for use by state agencies.

(h) Upon request, assist state agencies in the development of information technology-related legislative budget requests.

(i) Conduct annual assessments of state agencies to determine compliance with all information technology standards and guidelines developed and published by the Florida Digital Service ~~department~~ and provide results of the assessments to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives.

(j) Conduct a market analysis not less frequently than every 3 years beginning in 2021 to determine whether the information technology resources within the enterprise are utilized in the most cost-effective and cost-efficient manner, while recognizing that the replacement of certain legacy information technology systems within the enterprise may be cost prohibitive or cost inefficient due to the remaining useful life of those resources; whether the enterprise is complying with the cloud-first policy specified in s. 282.206; and whether the enterprise is utilizing best practices with respect to information technology, information services, and the acquisition of emerging technologies and information services. Each market analysis shall be used to prepare a strategic plan for continued and future information technology and information

services for the enterprise, including, but not limited to, proposed acquisition of new services or technologies and approaches to the implementation of any new services or technologies. Copies of each market analysis and accompanying strategic plan must be submitted to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives not later than December 31 of each year that a market analysis is conducted.

(k) Recommend other information technology services that should be designed, delivered, and managed as enterprise information technology services. Recommendations must include the identification of existing information technology resources associated with the services, if existing services must be transferred as a result of being delivered and managed as enterprise information technology services.

(l) In consultation with state agencies, propose a methodology and approach for identifying and collecting both current and planned information technology expenditure data at the state agency level.

(m)1. Notwithstanding any other law, provide project oversight on any information technology project of the Department of Financial Services, the Department of Legal Affairs, and the Department of Agriculture and Consumer Services which has a total project cost of $20 million or more. Such information technology projects must also comply with the

applicable information technology architecture, project management and oversight, and reporting standards established by the ~~department, acting through the~~ Florida Digital Service.

2. When performing the project oversight function specified in subparagraph 1., report at least quarterly to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives on any information technology project that the ~~department, acting through the~~ Florida Digital Service~~,~~ identifies as high-risk due to the project exceeding acceptable variance ranges defined and documented in the project plan. The report shall include a risk assessment, including fiscal risks, associated with proceeding to the next stage of the project and a recommendation for corrective actions required, including suspension or termination of the project.

(n) If an information technology project implemented by a state agency must be connected to or otherwise accommodated by an information technology system administered by the Department of Financial Services, the Department of Legal Affairs, or the Department of Agriculture and Consumer Services, consult with these departments regarding the risks and other effects of such projects on their information technology systems and work cooperatively with these departments regarding the connections, interfaces, timing, or accommodations required to implement such projects.

(o) If adherence to standards or policies adopted by or established pursuant to this section causes conflict with federal regulations or requirements imposed on an entity within the enterprise and results in adverse action against an entity or federal funding, work with the entity to provide alternative standards, policies, or requirements that do not conflict with the federal regulation or requirement. The ~~department, acting through the~~ Florida Digital Service~~,~~ shall annually report such alternative standards to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives.

(p)1. Establish an information technology policy for all information technology-related state contracts, including state term contracts for information technology commodities, consultant services, and staff augmentation services. The information technology policy must include:

a. Identification of the information technology product and service categories to be included in state term contracts.

b. Requirements to be included in solicitations for state term contracts.

c. Evaluation criteria for the award of information technology-related state term contracts.

d. The term of each information technology-related state term contract.

e. The maximum number of vendors authorized on each state

term contract.

f. At a minimum, a requirement that any contract for information technology commodities or services meet the National Institute of Standards and Technology Cybersecurity Framework.

g. For an information technology project wherein project oversight is required pursuant to paragraph (d) or paragraph (m), a requirement that independent verification and validation be employed throughout the project life cycle with the primary objective of independent verification and validation being to provide an objective assessment of products and processes throughout the project life cycle. An entity providing independent verification and validation may not have technical, managerial, or financial interest in the project and may not have responsibility for, or participate in, any other aspect of the project.

2. Evaluate vendor responses for information technology-related state term contract solicitations and invitations to negotiate.

3. Answer vendor questions on information technology-related state term contract solicitations.

4. Ensure that the information technology policy established pursuant to subparagraph 1. is included in all solicitations and contracts that are administratively executed by the department.

(q) Recommend potential methods for standardizing data

across state agencies which will promote interoperability and reduce the collection of duplicative data.

(r) Recommend open data technical standards and terminologies for use by the enterprise.

(s) Ensure that enterprise information technology solutions are capable of utilizing an electronic credential and comply with the enterprise architecture standards.

(t) Establish an operations committee that shall meet as necessary for the purpose of developing collaborative efforts between agencies and other governmental entities relating to cybersecurity issues, including the coordination of response efforts relating to cybersecurity incidents and issues relating to the interoperability of agency projects. The state chief information security officer shall serve as the executive director of the committee. The committee shall be composed of the following members:

1. The Attorney General, or his or her designee.

2. The Secretary of State, or his or her designee.

3. The executive director of the Department of Law Enforcement, or his or her designee.

4. A representative of each state agency.

5. A representative of the Florida State Guard.

6. A representative of the Florida National Guard.

(2)(a) The Governor shall appoint ~~Secretary of Management Services shall designate~~ a state chief information officer,

subject to confirmation by the Senate, who shall administer the Florida Digital Service. The state chief information officer, before ~~prior to~~ appointment, must have at least 5 years of experience in the development of information system strategic planning and development or information technology policy, and, preferably, have leadership-level experience in the design, development, and deployment of interoperable software and data solutions.

(b) The state chief information officer~~, in consultation with the Secretary of Management Services,~~ shall designate a state chief data officer. The chief data officer must be a proven and effective administrator who must have significant and substantive experience in data management, data governance, interoperability, and security.

(3) The ~~department, acting through the~~ Florida Digital Service, ~~and~~ from funds appropriated to the Florida Digital Service, shall:

(a) Create~~, not later than December 1, 2022,~~ and maintain a comprehensive indexed data catalog in collaboration with the enterprise that lists the data elements housed within the enterprise and the legacy system or application in which these data elements are located. The data catalog must, at a minimum, specifically identify all data that is restricted from public disclosure based on federal or state laws and regulations and require that all such information be protected in accordance

with s. 282.318.

(b) Develop and publish~~, not later than December 1, 2022,~~ in collaboration with the enterprise, a data dictionary for each agency that reflects the nomenclature in the comprehensive indexed data catalog.

(c) Adopt, by rule, standards that support the creation and deployment of an application programming interface to facilitate integration throughout the enterprise.

(d) Adopt, by rule, standards necessary to facilitate a secure ecosystem of data interoperability that is compliant with the enterprise architecture.

(e) Adopt, by rule, standards that facilitate the deployment of applications or solutions to the existing enterprise system in a controlled and phased approach.

(f) After submission of documented use cases developed in conjunction with the affected agencies, assist the affected agencies with the deployment, contingent upon a specific appropriation therefor, of new interoperable applications and solutions:

1. For the Department of Health, the Agency for Health Care Administration, the Agency for Persons with Disabilities, the Department of Education, the Department of Elderly Affairs, and the Department of Children and Families.

2. To support military members, veterans, and their families.

(4) For information technology projects that have ~~a~~ total project costs ~~cost~~ of $5 ~~$10~~ million or more:

(a) State agencies must provide the Florida Digital Service with written notice of any planned procurement of an information technology project.

(b) The Florida Digital Service must participate in the development of specifications and recommend modifications to any planned procurement of an information technology project by state agencies so that the procurement complies with the enterprise architecture.

(c) The Florida Digital Service must participate in post-award contract monitoring.

(5) The department, acting through the Florida Digital Service, may not retrieve or disclose any data without a shared-data agreement in place between the department and the enterprise entity that has primary custodial responsibility of, or data-sharing responsibility for, that data.

(6) The ~~department, acting through the~~ Florida Digital Service~~,~~ shall adopt rules to administer this section.

Section 4. Section 282.201, Florida Statutes, is amended to read:

282.201 State data center.—The state data center is established within the department and shall be overseen by the Florida Digital Service. The provision of data center services must comply with applicable state and federal laws, regulations,

and policies, including all applicable security, privacy, and auditing requirements. The Florida Digital Service ~~department~~ shall appoint a director of the state data center who has experience in leading data center facilities and has expertise in cloud-computing management. The Florida Digital Service shall be provided with full access to state data center infrastructure.

(1) STATE DATA CENTER DUTIES.—The state data center shall:

(a) Offer, develop, and support the services and applications defined in service-level agreements executed with its customer entities.

(b) Maintain performance of the state data center by ensuring proper data backup; data backup recovery; disaster recovery; and appropriate security, power, cooling, fire suppression, and capacity.

(c) Develop and implement business continuity and disaster recovery plans, and annually conduct a live exercise of each plan.

(d) Enter into a service-level agreement with each customer entity to provide the required type and level of service or services. If a customer entity fails to execute an agreement within 60 days after commencement of a service, the state data center may cease service. A service-level agreement may not have a term exceeding 3 years and at a minimum must:

1. Identify the parties and their roles, duties, and

responsibilities under the agreement.

2. State the duration of the contract term and specify the conditions for renewal.

3. Identify the scope of work.

4. Identify the products or services to be delivered with sufficient specificity to permit an external financial or performance audit.

5. Establish the services to be provided, the business standards that must be met for each service, the cost of each service by agency application, and the metrics and processes by which the business standards for each service are to be objectively measured and reported.

6. Provide a timely billing methodology to recover the costs of services provided to the customer entity pursuant to s. 215.422.

7. Provide a procedure for modifying the service-level agreement based on changes in the type, level, and cost of a service.

8. Include a right-to-audit clause to ensure that the parties to the agreement have access to records for audit purposes during the term of the service-level agreement.

9. Provide that a service-level agreement may be terminated by either party for cause only after giving the other party and the Florida Digital Service ~~department~~ notice in writing of the cause for termination and an opportunity for the

other party to resolve the identified cause within a reasonable period.

10. Provide for mediation of disputes by the Division of Administrative Hearings pursuant to s. 120.573.

(e) For purposes of chapter 273, be the custodian of resources and equipment located in and operated, supported, and managed by the state data center.

(f) Assume administrative access rights to resources and equipment, including servers, network components, and other devices, consolidated into the state data center.

1. Upon consolidation, a state agency shall relinquish administrative rights to consolidated resources and equipment. State agencies required to comply with federal and state criminal justice information security rules and policies shall retain administrative access rights sufficient to comply with the management control provisions of those rules and policies; however, the state data center shall have the appropriate type or level of rights to allow the center to comply with its duties pursuant to this section. The Department of Law Enforcement shall serve as the arbiter of disputes pertaining to the appropriate type and level of administrative access rights pertaining to the provision of management control in accordance with the federal criminal justice information guidelines.

2. The state data center shall provide customer entities with access to applications, servers, network components, and

other devices necessary for entities to perform business activities and functions, and as defined and documented in a service-level agreement.

(g) In its procurement process, show preference for cloud-computing solutions that minimize or do not require the purchasing, financing, or leasing of state data center infrastructure, and that meet the needs of customer agencies, that reduce costs, and that meet or exceed the applicable state and federal laws, regulations, and standards for cybersecurity.

(h) Assist customer entities in transitioning from state data center services to the Northwest Regional Data Center or other third-party cloud-computing services procured by a customer entity or by the Northwest Regional Data Center on behalf of a customer entity.

(2) USE OF THE STATE DATA CENTER.—The following are exempt from the use of the state data center: the Department of Law Enforcement, the Department of the Lottery's Gaming System, Systems Design and Development in the Office of Policy and Budget, the regional traffic management centers as described in s. 335.14(2) and the Office of Toll Operations of the Department of Transportation, the State Board of Administration, state attorneys, public defenders, criminal conflict and civil regional counsel, capital collateral regional counsel, and the Florida Housing Finance Corporation.

(3) AGENCY LIMITATIONS.—Unless exempt from the use of the

state data center pursuant to this section or authorized by the Legislature, a state agency may not:

(a) Create a new agency computing facility or data center, or expand the capability to support additional computer equipment in an existing agency computing facility or data center; or

(b) Terminate services with the state data center without giving written notice of intent to terminate services 180 days before such termination.

(4) FLORIDA DIGITAL SERVICE ~~DEPARTMENT~~ RESPONSIBILITIES.—The Florida Digital Service ~~department~~ shall provide operational management and oversight of the state data center, which includes:

(a) Implementing industry standards and best practices for the state data center's facilities, operations, maintenance, planning, and management processes.

(b) Developing and implementing cost-recovery mechanisms that recover the full direct and indirect cost of services through charges to applicable customer entities. Such cost-recovery mechanisms must comply with applicable state and federal regulations concerning distribution and use of funds and must ensure that, for any fiscal year, no service or customer entity subsidizes another service or customer entity. The Florida Digital Service ~~department~~ may recommend other payment mechanisms to the Executive Office of the Governor, the

President of the Senate, and the Speaker of the House of Representatives. Such mechanisms may be implemented only if specifically authorized by the Legislature.

(c) Developing and implementing appropriate operating guidelines and procedures necessary for the state data center to perform its duties pursuant to subsection (1). The guidelines and procedures must comply with applicable state and federal laws, regulations, and policies and conform to generally accepted governmental accounting and auditing standards. The guidelines and procedures must include, but need not be limited to:

1. Implementing a consolidated administrative support structure responsible for providing financial management, procurement, transactions involving real or personal property, human resources, and operational support.

2. Implementing an annual reconciliation process to ensure that each customer entity is paying for the full direct and indirect cost of each service as determined by the customer entity's use of each service.

3. Providing rebates that may be credited against future billings to customer entities when revenues exceed costs.

4. Requiring customer entities to validate that sufficient funds exist before implementation of a customer entity's request for a change in the type or level of service provided, if such change results in a net increase to the customer entity's cost

for that fiscal year.

5. By November 15 of each year, providing to the Office of Policy and Budget in the Executive Office of the Governor and to the chairs of the legislative appropriations committees the projected costs of providing data center services for the following fiscal year.

6. Providing a plan for consideration by the Legislative Budget Commission if the cost of a service is increased for a reason other than a customer entity's request made pursuant to subparagraph 4. Such a plan is required only if the service cost increase results in a net increase to a customer entity for that fiscal year.

7. Standardizing and consolidating procurement and contracting practices.

(d) In collaboration with the Department of Law Enforcement and the Florida Digital Service, developing and implementing a process for detecting, reporting, and responding to cybersecurity incidents, breaches, and threats.

(e) Adopting rules relating to the operation of the state data center, including, but not limited to, budgeting and accounting procedures, cost-recovery methodologies, and operating procedures.

(5) NORTHWEST REGIONAL DATA CENTER CONTRACT.—In order for the Florida Digital Service ~~department~~ to carry out its duties and responsibilities relating to the state data center, the

state chief information officer shall assume responsibility for the contract entered into by the secretary of the department ~~shall contract by July 1, 2022,~~ with the Northwest Regional Data Center pursuant to s. 287.057(11). The contract shall provide that the Northwest Regional Data Center will manage the operations of the state data center and provide data center services to state agencies. Notwithstanding the terms of the contract, the Northwest Regional Data Center must provide the Florida Digital Service with access to information regarding the operations of the state data center.

(a) The Florida Digital Service ~~department~~ shall provide contract oversight, including, but not limited to, reviewing invoices provided by the Northwest Regional Data Center for services provided to state agency customers.

(b) The Florida Digital Service ~~department~~ shall approve or request updates to invoices within 10 business days after receipt. If the Florida Digital Service ~~department~~ does not respond to the Northwest Regional Data Center, the invoice will be approved by default. The Northwest Regional Data Center must submit approved invoices directly to state agency customers.

Section 5. Subsection (10) of section 282.318, Florida Statutes, is renumbered as subsection (11), subsections (3), (4), and (7) and present subsection (10) are amended, and a new subsection (10) is added to that section, to read:

282.318 Cybersecurity.—

(3) The ~~department, 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. Such standards and processes must be consistent with generally accepted technology best practices, including the National Institute for Standards and Technology Cybersecurity Framework, for cybersecurity. The ~~department, acting through the~~ Florida Digital Service~~,~~ shall adopt rules that mitigate risks; safeguard state agency digital assets, data, information, and information technology resources to ensure availability, confidentiality, and integrity; and support a security governance framework. The ~~department, acting through the~~ Florida Digital Service~~,~~ shall also:

(a) Designate an employee of the Florida Digital Service as the state chief information security officer. The state chief information security officer must have experience and expertise in security and risk management for communications and information technology resources. The state chief information security officer is responsible for the development, operation, and oversight of cybersecurity for state technology systems. The state chief information security officer shall be notified of all confirmed or suspected incidents or threats of state agency information technology resources and must report such incidents or threats to the state chief information officer and the

Governor.

(b) Develop, and annually update by February 1, a statewide cybersecurity strategic plan that includes security goals and objectives for cybersecurity, including the identification and mitigation of risk, proactive protections against threats, tactical risk detection, threat reporting, and response and recovery protocols for a cyber incident.

(c) Develop and publish for use by state agencies a cybersecurity governance framework that, at a minimum, includes guidelines and processes for:

1. Establishing asset management procedures to ensure that an agency's information technology resources are identified and managed consistent with their relative importance to the agency's business objectives.

2. Using a standard risk assessment methodology that includes the identification of an agency's priorities, constraints, risk tolerances, and assumptions necessary to support operational risk decisions.

3. Completing comprehensive risk assessments and cybersecurity audits, which may be completed by a private sector vendor, and submitting completed assessments and audits to the Florida Digital Service. The Florida Digital Service shall oversee any cybersecurity audit completed by a private sector vendor to ensure that the audit meets applicable standards, processes, and timelines ~~department~~.

4. Identifying protection procedures to manage the protection of an agency's information, data, and information technology resources.

5. Establishing procedures for accessing information and data to ensure the confidentiality, integrity, and availability of such information and data.

6. Detecting threats through proactive monitoring of events, continuous security monitoring, and defined detection processes.

7. Establishing agency cybersecurity incident response teams and describing their responsibilities for responding to cybersecurity incidents, including breaches of personal information containing confidential or exempt data.

8. Recovering information and data in response to a cybersecurity incident. The recovery may include recommended improvements to the agency processes, policies, or guidelines.

9. Establishing a cybersecurity incident reporting process that includes procedures for notifying the Florida Digital Service ~~department~~ and the Department of Law Enforcement of cybersecurity incidents.

a. The level of severity of the cybersecurity incident is defined by the National Cyber Incident Response Plan of the United States Department of Homeland Security as follows:

(I) Level 5 is an emergency-level incident within the specified jurisdiction that poses an imminent threat to the

provision of wide-scale critical infrastructure services; national, state, or local government security; or the lives of the country's, state's, or local government's residents.

(II) Level 4 is a severe-level incident that is likely to result in a significant impact in the affected jurisdiction to public health or safety; national, state, or local security; economic security; or civil liberties.

(III) Level 3 is a high-level incident that is likely to result in a demonstrable impact in the affected jurisdiction to public health or safety; national, state, or local security; economic security; civil liberties; or public confidence.

(IV) Level 2 is a medium-level incident that may impact public health or safety; national, state, or local security; economic security; civil liberties; or public confidence.

(V) Level 1 is a low-level incident that is unlikely to impact public health or safety; national, state, or local security; economic security; civil liberties; or public confidence.

b. The cybersecurity incident reporting process must specify the information that must be reported by a state agency following a cybersecurity incident or ransomware incident, which, at a minimum, must include the following:

(I) A summary of the facts surrounding the cybersecurity incident or ransomware incident.

(II) The date on which the state agency most recently

backed up its data; the physical location of the backup, if the backup was affected; and if the backup was created using cloud computing.

(III) The types of data compromised by the cybersecurity incident or ransomware incident.

(IV) The estimated fiscal impact of the cybersecurity incident or ransomware incident.

(V) In the case of a ransomware incident, the details of the ransom demanded.

c.(I) A state agency shall report all ransomware incidents and ~~any~~ cybersecurity incidents ~~incident determined by the state agency to be of severity level 3, 4, or 5~~ to the Florida Digital Service, the Cybersecurity Operations Center, and the Cybercrime Office of the Department of Law Enforcement as soon as possible but no later than 4 ~~48~~ hours after discovery of the cybersecurity incident and no later than 2 ~~12~~ hours after discovery of the ransomware incident. The report must contain the information required in sub-subparagraph b. The Florida Digital Service shall notify the Governor, the President of the Senate, and the Speaker of the House of Representatives of any incident discovered by a state agency but not timely reported under this sub-sub-subparagraph.

(II) The Cybersecurity Operations Center shall notify the President of the Senate and the Speaker of the House of Representatives of any severity level 3, 4, or 5 incident as

soon as possible but no later than 12 hours after receiving a state agency's incident report. The notification must include a high-level description of the incident and the likely effects and must be provided in a secure environment.

d. ~~A state agency shall report a cybersecurity incident determined by the state agency to be of severity level 1 or 2 to the Cybersecurity Operations Center and the Cybercrime Office of the Department of Law Enforcement as soon as possible. The report must contain the information required in sub-subparagraph b.~~

~~e.~~ The Cybersecurity Operations Center shall provide a consolidated incident report on a quarterly basis to the President of the Senate, the Speaker of the House of Representatives, and the Florida Cybersecurity Advisory Council. The report provided to the Florida Cybersecurity Advisory Council may not contain the name of any agency, network information, or system identifying information but must contain sufficient relevant information to allow the Florida Cybersecurity Advisory Council to fulfill its responsibilities as required in s. 282.319(9).

10. Incorporating information obtained through detection and response activities into the agency's cybersecurity incident response plans.

11. Developing agency strategic and operational cybersecurity plans required pursuant to this section.

12. Establishing the managerial, operational, and technical safeguards for protecting state government data and information technology resources that align with the state agency risk management strategy and that protect the confidentiality, integrity, and availability of information and data.

13. Establishing procedures for procuring information technology commodities and services that require the commodity or service to meet the National Institute of Standards and Technology Cybersecurity Framework.

14. Submitting after-action reports following a cybersecurity incident or ransomware incident. Such guidelines and processes for submitting after-action reports must be developed and published by December 1, 2022.

(d) Assist state agencies in complying with this section.

(e) In collaboration with the Cybercrime Office of the Department of Law Enforcement, annually provide training for state agency information security managers and computer security incident response team members that contains training on cybersecurity, including cybersecurity threats, trends, and best practices.

(f) Annually review the strategic and operational cybersecurity plans of state agencies.

(g) Annually provide cybersecurity training to all state agency technology professionals and employees with access to

highly sensitive information which develops, assesses, and documents competencies by role and skill level. The cybersecurity training curriculum must include training on the identification of each cybersecurity incident severity level referenced in sub-subparagraph (c)9.a. The training may be provided in collaboration with the Cybercrime Office of the Department of Law Enforcement, a private sector entity, or an institution of the State University System.

(h) Operate and maintain a Cybersecurity Operations Center led by the state chief information security officer, which must be primarily virtual and staffed with tactical detection and incident response personnel. The Cybersecurity Operations Center shall serve as a clearinghouse for threat information and coordinate with the Department of Law Enforcement to support state agencies and their response to any confirmed or suspected cybersecurity incident.

(i) Lead an Emergency Support Function, ESF CYBER, under the state comprehensive emergency management plan as described in s. 252.35.

(j) Provide cybersecurity briefings to the members of any legislative committee or subcommittee responsible for policy matters relating to cybersecurity.

(k) Have the authority to respond to any state agency cybersecurity incident.

(4) Each state agency head shall, at a minimum:

(a) Designate an information security manager to administer the cybersecurity program of the state agency. This designation must be provided annually in writing to the Florida Digital Service ~~department~~ by January 1. A state agency's information security manager, for purposes of these information security duties, shall report directly to the agency head.

(b) In consultation with the ~~department, through the~~ Florida Digital Service~~,~~ and the Cybercrime Office of the Department of Law Enforcement, establish an agency cybersecurity response team to respond to a cybersecurity incident. The agency cybersecurity response team shall convene upon notification of a cybersecurity incident and must immediately report all confirmed or suspected incidents to the state chief information security officer, or his or her designee, and comply with all applicable guidelines and processes established pursuant to paragraph (3)(c).

(c) Submit to the Florida Digital Service ~~department~~ annually by July 31, the state agency's strategic and operational cybersecurity plans developed pursuant to rules and guidelines established by the ~~department, through the~~ Florida Digital Service.

1. The state agency strategic cybersecurity plan must cover a 3-year period and, at a minimum, define security goals, intermediate objectives, and projected agency costs for the strategic issues of agency information security policy, risk

management, security training, security incident response, and disaster recovery. The plan must be based on the statewide cybersecurity strategic plan created by the Florida Digital Service ~~department~~ and include performance metrics that can be objectively measured to reflect the status of the state agency's progress in meeting security goals and objectives identified in the agency's strategic information security plan.

2. The state agency operational cybersecurity plan must include a progress report that objectively measures progress made towards the prior operational cybersecurity plan and a project plan that includes activities, timelines, and deliverables for security objectives that the state agency will implement during the current fiscal year.

(d) Conduct, and update every 3 years, a comprehensive risk assessment, which may be completed by a private sector vendor, to determine the security threats to the data, information, and information technology resources, including mobile devices and print environments, of the agency. The risk assessment must comply with the risk assessment methodology developed by the Florida Digital Service ~~department~~ and is confidential and exempt from s. 119.07(1), except that such information shall be available to the Auditor General, the Florida Digital Service ~~within the department~~, the Cybercrime Office of the Department of Law Enforcement, and, for state agencies under the jurisdiction of the Governor, the Chief

Inspector General. If a private sector vendor is used to complete a comprehensive risk assessment, it must attest to the validity of the risk assessment findings.

(e) Develop, and periodically update, written internal policies and procedures, which include procedures for reporting cybersecurity incidents and breaches to the Cybercrime Office of the Department of Law Enforcement and the Florida Digital Service ~~within the department~~. Such policies and procedures must be consistent with the rules, guidelines, and processes established by the Florida Digital Service ~~department~~ to ensure the security of the data, information, and information technology resources of the agency. The internal policies and procedures that, if disclosed, could facilitate the unauthorized modification, disclosure, or destruction of data or information technology resources are confidential information and exempt from s. 119.07(1), except that such information shall be available to the Auditor General, the Cybercrime Office of the Department of Law Enforcement, the Florida Digital Service ~~within the department~~, and, for state agencies under the jurisdiction of the Governor, the Chief Inspector General.

(f) Implement managerial, operational, and technical safeguards and risk assessment remediation plans recommended by the Florida Digital Service ~~department~~ to address identified risks to the data, information, and information technology resources of the agency. The ~~department, through the~~ Florida

Digital Service~~,~~ shall track implementation by state agencies upon development of such remediation plans in coordination with agency inspectors general.

(g) Ensure that periodic internal audits and evaluations of the agency's cybersecurity program for the data, information, and information technology resources of the agency are conducted. The results of such audits and evaluations are confidential information and exempt from s. 119.07(1), except that such information shall be available to the Auditor General, the Cybercrime Office of the Department of Law Enforcement, the Florida Digital Service ~~within the department~~, and, for agencies under the jurisdiction of the Governor, the Chief Inspector General.

(h) Ensure that the cybersecurity requirements in the written specifications for the solicitation, contracts, and service-level agreement of information technology and information technology resources and services meet or exceed the applicable state and federal laws, regulations, and standards for cybersecurity, including the National Institute of Standards and Technology Cybersecurity Framework. Service-level agreements must identify service provider and state agency responsibilities for privacy and security, protection of government data, personnel background screening, and security deliverables with associated frequencies.

(i) Provide cybersecurity awareness training to all state

agency employees within 30 days after commencing employment, and annually thereafter, concerning cybersecurity risks and the responsibility of employees to comply with policies, standards, guidelines, and operating procedures adopted by the state agency to reduce those risks. The training may be provided in collaboration with the Cybercrime Office of the Department of Law Enforcement, a private sector entity, or an institution of the State University System.

(j) Develop a process for detecting, reporting, and responding to threats, breaches, or cybersecurity incidents which is consistent with the security rules, guidelines, and processes established by the ~~department through the~~ Florida Digital Service.

1. All cybersecurity incidents and ransomware incidents must be reported by state agencies. Such reports must comply with the notification procedures and reporting timeframes established pursuant to paragraph (3)(c).

2. For cybersecurity breaches, state agencies shall provide notice in accordance with s. 501.171.

(k) Submit to the Florida Digital Service, within 1 week after the remediation of a cybersecurity incident or ransomware incident, an after-action report that summarizes the incident, the incident's resolution, and any insights gained as a result of the incident.

(7) The portions of records made confidential and exempt

in subsections (5) and (6) shall be available to the Auditor General, the Cybercrime Office of the Department of Law Enforcement, the Florida Digital Service ~~within the department~~, and, for agencies under the jurisdiction of the Governor, the Chief Inspector General. Such portions of records may be made available to a local government, another state agency, or a federal agency for cybersecurity purposes or in furtherance of the state agency's official duties.

(10) Any legislative committee or subcommittee responsible for policy matters relating to cybersecurity may hold meetings closed by the respective legislative body under the rules of such legislative body at which such committee or subcommittee is briefed on records made confidential and exempt under subsections (5) and (6). The committee or subcommittee must maintain the confidential and exempt status of such records.

(11) ~~(10)~~ The Florida Digital Service ~~department~~ shall adopt rules relating to cybersecurity and to administer this section.

Section 6. Paragraph (d) of subsection (5) of section 282.3185, Florida Statutes, is redesignated as paragraph (c), and paragraph (b) and present paragraph (c) of that subsection are amended to read:

282.3185 Local government cybersecurity.—

(5) INCIDENT NOTIFICATION.—

(b)1. A local government shall report all ransomware

incidents and ~~any~~ cybersecurity incidents ~~incident determined by the local government to be of severity level 3, 4, or 5~~ as provided in s. 282.318(3)(c) to the Florida Digital Service, the Cybersecurity Operations Center, the Cybercrime Office of the Department of Law Enforcement, and the sheriff who has jurisdiction over the local government as soon as possible but no later than 4 ~~48~~ hours after discovery of the cybersecurity incident and no later than 2 ~~12~~ hours after discovery of the ransomware incident. The report must contain the information required in paragraph (a). The Florida Digital Service shall notify the Governor, the President of the Senate, and the Speaker of the House of Representatives of any incident discovered by a local government but not timely reported under this subparagraph.

2. The Cybersecurity Operations Center shall notify the President of the Senate and the Speaker of the House of Representatives of any severity level 3, 4, or 5 incident as soon as possible but no later than 12 hours after receiving a local government's incident report. The notification must include a high-level description of the incident and the likely effects and must be provided in a secure environment.

~~(c) A local government may report a cybersecurity incident determined by the local government to be of severity level 1 or 2 as provided in s. 282.318(3)(c) to the Cybersecurity Operations Center, the Cybercrime Office of the Department of~~

~~Law Enforcement, and the sheriff who has jurisdiction over the local government. The report shall contain the information required in paragraph (a).~~

Section 7. Subsections (10) through (13) of section 282.319, Florida Statutes, are renumbered as subsections (11) through (14), respectively, paragraph (j) of subsection (4) and subsection (6) are amended, and a new subsection (10) is added to that section, to read:

282.319 Florida Cybersecurity Advisory Council.—

(4) The council shall be comprised of the following members:

(j) Three representatives from critical infrastructure sectors, ~~one of whom must be from a water treatment facility,~~ appointed by the Governor.

(6) The state chief information officer ~~Secretary of Management Services~~, or his or her designee, shall serve as the ex officio, nonvoting executive director of the council.

(10) Members of any legislative committee or subcommittee responsible for policy matters relating to cybersecurity must be invited to and may attend meetings of the council. A council meeting at which two or more members of the Legislature are in attendance may not be construed as a meeting of a legislative committee or subcommittee or as a prearranged gathering between more than two members of the Legislature, the purpose of which is to agree upon formal legislative action that will be taken at

a subsequent time.

Section 8. Section 282.3195, Florida Statutes, is created to read:

282.3195 State Technology Advancement Council.—

(1) The State Technology Advancement Council, an advisory council as defined in s. 20.03(7), is created within the Executive Office of the Governor. Except as otherwise provided in this section, the advisory council shall operate in a manner consistent with s. 20.052.

(2) The purpose of the council is to:

(a) Assist state agencies and advise the Legislature on innovative technologies.

(b) Improve state technology project timelines.

(c) Develop efficient state technology processes.

(d) Assist in the creation of development and testing environments that allow state entities to proof technology concepts before engaging in procurement and otherwise develop processes to reduce wasteful spending on inappropriate technology.

(e) Assist Florida College System institutions and state universities with technology transfer processes.

(f) Support research on and development of innovative technologies.

(3) The state chief information officer, or his or her designee, shall serve as the executive director of the council.

The council shall be comprised of the following members appointed by the Governor:

(a) A person with senior level experience in cloud computing technology.

(b) An engineer.

(c) A person with senior level experience in the space industry.

(d) A data scientist.

(e) Other persons with relevant experience as determined by the Governor.

(4) Members shall serve for terms of 4 years; however, for the purpose of providing staggered terms, the initial appointments of two members shall be for terms of 2 years. A vacancy shall be filled for the remainder of the unexpired term in the same manner as the initial appointment. All members of the council are eligible for reappointment.

(5) The state chief information officer shall serve as the ex officio, nonvoting executive director of the council.

(6) Members shall serve without compensation but are entitled to receive reimbursement for per diem and travel expenses pursuant to s. 112.061.

(7) Members of the council shall maintain the confidential or exempt status of information received in the performance of their duties and responsibilities as members of the council. In accordance with s. 112.313, a current or former member of the

council may not disclose or use information not available to the general public and gained by reason of his or her official position, except for information relating exclusively to governmental practices, for his or her personal gain or benefit or for the personal gain or benefit of any other person or business entity. Members shall sign an agreement acknowledging the provisions of this subsection.

(8) The council shall meet at least quarterly.

(9) Beginning June 1, 2024, and annually on June 1 thereafter, the council shall submit to the Governor, the President of the Senate, and the Speaker of the House of Representatives a report describing the activities of the council and providing recommendations as appropriate.

Section 9. Section 768.401, Florida Statutes, is created to read:

768.401 Limitation on liability for cybersecurity incidents.—

(1) A county or municipality that substantially complies with s. 282.3185 shall gain a presumption against liability in connection with a cybersecurity incident.

(2) A sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information shall gain a presumption against liability in connection with a cybersecurity incident if the entity

substantially complies with s. 501.171, if applicable, and has:

(a) Adopted a cybersecurity program that substantially aligns with the current version of any of the following:

1. The National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity.

2. NIST special publication 800-171.

3. NIST special publications 800-53 and 800-53A.

4. The Federal Risk and Authorization Management Program security assessment framework.

5. CIS Critical Security Controls.

6. The International Organization for Standardization/International Electrotechnical Commission 27000-series family of standards; or

(b) If regulated by the state or Federal Government, or both, or if otherwise subject to the requirements of any of the following laws and regulations, substantially complied its cybersecurity program to the current version of the following, as applicable:

1. The security requirements of the Health Insurance Portability and Accountability Act of 1996, 45 C.F.R. part 164 subpart C.

2. Title V of the Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, as amended.

3. The Federal Information Security Modernization Act of

2014, Pub. L. No. 113-283.

4. The Health Information Technology for Economic and Clinical Health Act, 45 C.F.R. part 162.

(3) A commercial entity that substantially complies with a combination of industry-recognized cybersecurity frameworks or standards, including the payment card industry data security standard, to gain the presumption against liability pursuant to subsection (2) must, upon the revision of two or more of the frameworks or standards with which the entity complies, adopt the revised frameworks or standards within 1 year after the latest publication date stated in the revisions.

(4) This section does not establish a private cause of action. Failure of a county, municipality, or commercial entity to substantially implement a cybersecurity program that is in compliance with this section is not evidence of negligence and does not constitute negligence per se.

Section 10. Paragraph (k) of subsection (1) of section 1004.649, Florida Statutes, is amended to read:

1004.649 Northwest Regional Data Center.—

(1) For the purpose of providing data center services to its state agency customers, the Northwest Regional Data Center is designated as a state data center for all state agencies and shall:

(k) Prepare and submit state agency customer invoices to the Florida Digital Service ~~Department of Management Services~~

for approval. Upon approval or by default pursuant to s. 282.201(5), submit invoices to state agency customers.

Section 11. This act shall take effect July 1, 2023.

# Energy, Communications & Cybersecurity Subcommittee
# HB 1511 by Rep. Giallombardo
# Cybersecurity

## AMENDMENT SUMMARY
## March 21, 2023

---

**Amendment 1 by Rep. Giallombardo (strike-all):**

- Removes language from the bill that shifted authority related to cybersecurity governance from the Department of Management Services (DMS) to the Florida Digital Service (FLDS).
- Clarifies, adds, and removes definitions.
- Removes language that lowered the reporting and oversight requirement for technology projects.
- Gives DMS additional responsibilities for technology project oversight and provides what oversight entails.
- Changes the date DMS, acting through FLDS, must provide recommendations for standardization and consolidation of information technology services that support interoperability and cloud-first policy.
- Specifies that the quarterly report for project oversight must be submitted by the 15th day following the end of each quarter.
- Specifies a date that alternative standards are due, if applicable.
- Changes the members of the operations committee created by the bill.
- Requires the state chief information officer to designate a state chief technology officer and outlines the responsibilities of the position.
- Requires the entity assuming the responsibilities of the State Data Center (SDC) to fully integrate with the Cybersecurity Operations Center.
- Specifies what information the SDC must report to DMS and FLDS.
- Requires that FLDS submit an annual comprehensive risk assessment facilitated by DMS and includes criteria for this assessment.
- Removes the State Technology Advancement Council created by the bill.
- Creates an exemption to the requirements of ch. 110 relating to state employment for personnel employed by or reporting to certain officers.
- Clarifies application of a presumption against liability.

COMMITTEE/SUBCOMMITTEE ACTION

| | |
|---|---|
| ADOPTED | ___ (Y/N) |
| ADOPTED AS AMENDED | ___ (Y/N) |
| ADOPTED W/O OBJECTION | ___ (Y/N) |
| FAILED TO ADOPT | ___ (Y/N) |
| WITHDRAWN | ___ (Y/N) |
| OTHER | _____ |

Committee/Subcommittee hearing bill: Energy, Communications & Cybersecurity Subcommittee

Representative Giallombardo offered the following:

**Amendment (with title amendment)**

Remove everything after the enacting clause and insert:

Section 1. This act may be cited as the "Florida Cyber Protection Act."

Section 2. Paragraph (y) is added to subsection (2) of section 110.205, Florida Statutes, to read:

110.205 Career service; exemptions.—

(2) EXEMPT POSITIONS.—The exempt positions that are not covered by this part include the following:

(y) Personnel employed by or reporting to the state chief information security officer, the state chief data officer, a chief information security officer, and an agency information

security manager.

Section 3. Subsections (3) through (5), (6) through (19), and (20) through (38) of section 282.0041, Florida Statutes, are renumbered as subsections (4) through (6), (8) through (21), and (24) through (42), respectively, present subsection (19) is amended, and new subsections (3), (7), (22), and (23) are added to that section, to read:

282.0041 Definitions.—As used in this chapter, the term:

(3) "As a service" means the contracting with or outsourcing to a third-party of a defined role or function as a means of delivery.

(7) "Cloud provider" has the same meaning as provided in Special Publication 800-145 issued by the National Institute of Standards and Technology.

(21)~~(19)~~ "Incident" means a violation or an imminent threat of violation, whether such violation is accidental or deliberate, of information technology resources, security, policies, or practices, or which may jeopardize the confidentiality, integrity, or availability of an information technology system or the information the system processes, stores, or transmits. An imminent threat of violation refers to a situation in which a state agency, county, or municipality has a factual basis for believing that a specific incident is about to occur.

(22) "Independent" means, for an entity providing

independent verification and validation, having no technical, managerial, or financial interest in the relevant technology project; no relationship to the relevant agency; and no responsibility for or participation in any aspect of the project, which includes project oversight by the Florida Digital Service.

(23) "Independent verification and validation" means third-party support services that provide a completely independent and impartial assessment of the progress and work products of a technology project from concept to business case and throughout the project lifecycle.

Section 4. Section 282.0051, Florida Statutes, is amended to read:

282.0051 Department of Management Services; Florida Digital Service; powers, duties, and functions.—

(1) The Florida Digital Service is ~~has been~~ created within the department to propose innovative solutions that securely modernize state government, including technology and information services, to achieve value through digital transformation and interoperability, and to fully support the cloud-first policy as specified in s. 282.206. The department, through the Florida Digital Service, shall have the following powers, duties, and functions:

(a) Develop and publish information technology policy for the management of the state's information technology resources.

(b) Develop an enterprise architecture that:

1. Acknowledges the unique needs of the entities within the enterprise in the development and publication of standards and terminologies to facilitate digital interoperability;

2. Supports the cloud-first policy as specified in s. 282.206; and

3. Addresses how information technology infrastructure may be modernized to achieve cloud-first objectives.

(c) Establish project management and oversight standards with which state agencies must comply when implementing information technology projects. The department, acting through the Florida Digital Service, shall provide training opportunities to state agencies to assist in the adoption of the project management and oversight standards. To support data-driven decisionmaking, the standards must include, but are not limited to:

1. Performance measurements and metrics that objectively reflect the status of an information technology project based on a defined and documented project scope, cost, and schedule.

2. Methodologies for calculating acceptable variances in the projected versus actual scope, schedule, or cost of an information technology project.

3. Reporting requirements, including requirements designed to alert all defined stakeholders that an information technology project has exceeded acceptable variances defined and documented

in a project plan.

4. Content, format, and frequency of project updates.

5. Technical standards to ensure an information technology project complies with the enterprise architecture.

(d) Ensure that independent ~~Perform~~ project oversight on all state agency information technology projects that have total project costs of $10 million or more and that are funded in the General Appropriations Act or any other law is performed and in compliance with applicable state and federal law.

1. The department may not be considered independent for purposes of project oversight under this paragraph on a project for which the department has provided or may be asked to provide any operational or technical support, including, but not limited to, providing advice or conducting any review.

2. The department shall establish an appropriate contract vehicle to facilitate procurement of project oversight as a service by the enterprise and ensure that the contract vehicle includes offerings that incorporate the ability to comply with applicable state and federal law, including any independent verification and validation requirements. An entity that provides project oversight as a service must provide a project oversight report to the department.

3. An agency may request the department to procure project oversight as a service for a project that is subject to this paragraph. Such procurement by the department does not violate

the requirement that the project oversight must be independent.

4. The department, acting through the Florida Digital Service, shall at least quarterly review received project oversight reports and, upon acceptance of the contents of such reports, provide the reports to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives.

5. The department, acting through the Florida Digital Service, shall report at least quarterly to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives on any information technology project that the department identifies as high-risk due to the project exceeding acceptable variance ranges defined and documented in a project plan. The report must include a risk assessment, including fiscal risks, associated with proceeding to the next stage of the project, and a recommendation for corrective actions required, including suspension or termination of the project.

(e) Identify opportunities for standardization and consolidation of information technology services that support interoperability and the cloud-first policy, as specified in s. 282.206, and business functions and operations, including administrative functions such as purchasing, accounting and reporting, cash management, and personnel, and that are common across state agencies. The department, acting through the

Florida Digital Service, shall biennially on January 15 ~~1~~ of each even-numbered year provide recommendations for standardization and consolidation to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives.

(f) Establish best practices for the procurement of information technology products and cloud-computing services in order to reduce costs, increase the quality of data center services, or improve government services.

(g) Develop standards for information technology reports and updates, including, but not limited to, operational work plans, project spend plans, and project status reports, for use by state agencies.

(h) Upon request, assist state agencies in the development of information technology-related legislative budget requests.

(i) Conduct annual assessments of state agencies to determine compliance with all information technology standards and guidelines developed and published by the department and provide results of the assessments to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives.

(j) Conduct a market analysis not less frequently than every 3 years beginning in 2021 to determine whether the information technology resources within the enterprise are utilized in the most cost-effective and cost-efficient manner,

while recognizing that the replacement of certain legacy information technology systems within the enterprise may be cost prohibitive or cost inefficient due to the remaining useful life of those resources; whether the enterprise is complying with the cloud-first policy specified in s. 282.206; and whether the enterprise is utilizing best practices with respect to information technology, information services, and the acquisition of emerging technologies and information services. Each market analysis shall be used to prepare a strategic plan for continued and future information technology and information services for the enterprise, including, but not limited to, proposed acquisition of new services or technologies and approaches to the implementation of any new services or technologies. Copies of each market analysis and accompanying strategic plan must be submitted to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives not later than December 31 of each year that a market analysis is conducted.

(k) Recommend other information technology services that should be designed, delivered, and managed as enterprise information technology services. Recommendations must include the identification of existing information technology resources associated with the services, if existing services must be transferred as a result of being delivered and managed as enterprise information technology services.

(l) In consultation with state agencies, propose a methodology and approach for identifying and collecting both current and planned information technology expenditure data at the state agency level.

(m)1. Notwithstanding any other law, provide project oversight on any information technology project of the Department of Financial Services, the Department of Legal Affairs, and the Department of Agriculture and Consumer Services which has a total project cost of $20 million or more. Such information technology projects must also comply with the applicable information technology architecture, project management and oversight, and reporting standards established by the department, acting through the Florida Digital Service.

2. When performing the project oversight function specified in subparagraph 1., report by the 15th day after the end of each quarter ~~at least quarterly~~ to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives on any information technology project that the department, acting through the Florida Digital Service, identifies as high-risk due to the project exceeding acceptable variance ranges defined and documented in the project plan. The report shall include a risk assessment, including fiscal risks, associated with proceeding to the next stage of the project and a recommendation for corrective actions required, including suspension or termination of the project.

(n) If an information technology project implemented by a state agency must be connected to or otherwise accommodated by an information technology system administered by the Department of Financial Services, the Department of Legal Affairs, or the Department of Agriculture and Consumer Services, consult with these departments regarding the risks and other effects of such projects on their information technology systems and work cooperatively with these departments regarding the connections, interfaces, timing, or accommodations required to implement such projects.

(o) If adherence to standards or policies adopted by or established pursuant to this section causes conflict with federal regulations or requirements imposed on an entity within the enterprise and results in adverse action against an entity or federal funding, work with the entity to provide alternative standards, policies, or requirements that do not conflict with the federal regulation or requirement. The department, acting through the Florida Digital Service, shall annually by January 15 report such alternative standards to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives.

(p)1. Establish an information technology policy for all information technology-related state contracts, including state term contracts for information technology commodities, consultant services, and staff augmentation services. The

information technology policy must include:

a. Identification of the information technology product and service categories to be included in state term contracts.

b. Requirements to be included in solicitations for state term contracts.

c. Evaluation criteria for the award of information technology-related state term contracts.

d. The term of each information technology-related state term contract.

e. The maximum number of vendors authorized on each state term contract.

f. At a minimum, a requirement that any contract for information technology commodities or services meet the National Institute of Standards and Technology Cybersecurity Framework.

g. For an information technology project wherein project oversight is required pursuant to paragraph (d) or paragraph (m), a requirement that independent verification and validation be employed throughout the project life cycle with the primary objective of independent verification and validation being to provide an objective assessment of products and processes throughout the project life cycle. An entity providing independent verification and validation may not have technical, managerial, or financial interest in the project and may not have responsibility for, or participate in, any other aspect of the project.

2. Evaluate vendor responses for information technology-related state term contract solicitations and invitations to negotiate.

3. Answer vendor questions on information technology-related state term contract solicitations.

4. Ensure that the information technology policy established pursuant to subparagraph 1. is included in all solicitations and contracts that are administratively executed by the department.

(q) Recommend potential methods for standardizing data across state agencies which will promote interoperability and reduce the collection of duplicative data.

(r) Recommend open data technical standards and terminologies for use by the enterprise.

(s) Ensure that enterprise information technology solutions are capable of utilizing an electronic credential and comply with the enterprise architecture standards.

(t) Establish an operations committee that shall meet as necessary for the purpose of developing collaborative efforts between agencies and other governmental entities relating to cybersecurity issues, including the coordination of preparedness and response efforts relating to cybersecurity incidents and issues relating to the interoperability of agency projects. The Secretary of Management Services shall serve as the executive director of the committee. The committee shall be composed of

the following members:

1. The state chief information officer, or his or her designee.

2. The Attorney General, or his or her designee.

3. The Secretary of State, or his or her designee.

4. The executive director of the Department of Law Enforcement, or his or her designee.

5. The Secretary of Transportation, or his or her designee.

6. The director of the Division of Emergency Management, or his or her designee.

7. The Secretary of Health Care Administration, or his or her designee.

8. The Commissioner of Education, or his or her designee.

9. The executive director of the Department of Highway Safety and Motor Vehicles, or his or her designee.

10. The chair of the Public Service Commission, or his or her designee.

11. The director of the Florida State Guard, or his or her designee.

12. The Adjutant General of the Florida National Guard, or his or her designee.

13. Any other agency head appointed by the Governor.

(2)(a) The Governor shall appoint ~~Secretary of Management Services shall designate~~ a state chief information officer,

subject to confirmation by the Senate, who shall administer the Florida Digital Service. The state chief information officer, before ~~prior to~~ appointment, must have at least 5 years of experience in the development of information system strategic planning and development or information technology policy, and, preferably, have leadership-level experience in the design, development, and deployment of interoperable software and data solutions.

(b) The state chief information officer~~, in consultation with the Secretary of Management Services,~~ shall designate a state chief data officer. The chief data officer must be a proven and effective administrator who must have significant and substantive experience in data management, data governance, interoperability, and security.

(c) The state chief information officer shall designate a state chief technology officer who shall be responsible for:

1. Exploring technology solutions to meet the enterprise need;

2. The deployments of adopted enterprise solutions;

3. Compliance with Florida's Cloud First policy;

4. Recommending best practices to increase the likelihood of technology project success;

5. Developing strategic partnerships with the private sector; and

6. Directly supporting enterprise cybersecurity and data

interoperability initiatives.

The chief cloud officer may acquire cloud migration as a service to comply with this section as it pertains to the implementation across the enterprise of Florida's Cloud First policy.

(3) The department, acting through the Florida Digital Service and from funds appropriated to the Florida Digital Service, shall:

(a) Create~~, not later than December 1, 2022,~~ and maintain a comprehensive indexed data catalog in collaboration with the enterprise that lists the data elements housed within the enterprise and the legacy system or application in which these data elements are located. The data catalog must, at a minimum, specifically identify all data that is restricted from public disclosure based on federal or state laws and regulations and require that all such information be protected in accordance with s. 282.318.

(b) Develop and publish~~, not later than December 1, 2022,~~ in collaboration with the enterprise, a data dictionary for each agency that reflects the nomenclature in the comprehensive indexed data catalog.

(c) Adopt, by rule, standards that support the creation and deployment of an application programming interface to facilitate integration throughout the enterprise.

(d) Adopt, by rule, standards necessary to facilitate a

secure ecosystem of data interoperability that is compliant with the enterprise architecture.

(e) Adopt, by rule, standards that facilitate the deployment of applications or solutions to the existing enterprise system in a controlled and phased approach.

(f) After submission of documented use cases developed in conjunction with the affected agencies, assist the affected agencies with the deployment, contingent upon a specific appropriation therefor, of new interoperable applications and solutions:

1. For the Department of Health, the Agency for Health Care Administration, the Agency for Persons with Disabilities, the Department of Education, the Department of Elderly Affairs, and the Department of Children and Families.

2. To support military members, veterans, and their families.

(4) For information technology projects that have ~~a~~ total project costs ~~cost~~ of $10 million or more:

(a) State agencies must provide the Florida Digital Service with written notice of any planned procurement of an information technology project.

(b) The Florida Digital Service must participate in the development of specifications and recommend modifications to any planned procurement of an information technology project by state agencies so that the procurement complies with the

enterprise architecture.

(c) The Florida Digital Service must participate in post-award contract monitoring.

(5) The department, acting through the Florida Digital Service, may not retrieve or disclose any data without a shared-data agreement in place between the department and the enterprise entity that has primary custodial responsibility of, or data-sharing responsibility for, that data.

(6) The department, acting through the Florida Digital Service, shall adopt rules to administer this section.

Section 5. Section 282.201, Florida Statutes, is amended to read:

282.201 State data center.—The state data center is established within the department and shall be overseen by and accountable to the department in consultation with the state chief information officer, the state chief data officer, the state chief information security officer, and the state chief technology officer. Any procurement or purchase of enterprise architecture which is comparable to a project that would be subject to requirements under s. 282.0051(4) if the total project cost was $10 million or more and which may be consumed by an enterprise must be provided to the department and the Florida Digital Service for review before publication. The provision of data center services must comply with applicable state and federal laws, regulations, and policies, including all

applicable security, privacy, and auditing requirements. The Florida Digital Service ~~department~~ shall appoint a director of the state data center who has experience in leading data center facilities and has expertise in cloud-computing management.

(1) STATE DATA CENTER DUTIES.—The state data center shall:

(a) Offer, develop, and support the services and applications defined in service-level agreements executed with its customer entities.

(b) Maintain performance of the state data center by ensuring proper data backup; data backup recovery; disaster recovery; and appropriate security, power, cooling, fire suppression, and capacity.

(c) Develop and implement business continuity and disaster recovery plans, and annually conduct a live exercise of each plan.

(d) Enter into a service-level agreement with each customer entity to provide the required type and level of service or services. If a customer entity fails to execute an agreement within 60 days after commencement of a service, the state data center may cease service. A service-level agreement may not have a term exceeding 3 years and at a minimum must:

1. Identify the parties and their roles, duties, and responsibilities under the agreement.

2. State the duration of the contract term and specify the conditions for renewal.

3. Identify the scope of work.

4. Identify the products or services to be delivered with sufficient specificity to permit an external financial or performance audit.

5. Establish the services to be provided, the business standards that must be met for each service, the cost of each service by agency application, and the metrics and processes by which the business standards for each service are to be objectively measured and reported.

6. Provide a timely billing methodology to recover the costs of services provided to the customer entity pursuant to s. 215.422.

7. Provide a procedure for modifying the service-level agreement based on changes in the type, level, and cost of a service.

8. Include a right-to-audit clause to ensure that the parties to the agreement have access to records for audit purposes during the term of the service-level agreement.

9. Provide that a service-level agreement may be terminated by either party for cause only after giving the other party and the department notice in writing of the cause for termination and an opportunity for the other party to resolve the identified cause within a reasonable period.

10. Provide for mediation of disputes by the Division of Administrative Hearings pursuant to s. 120.573.

(e) For purposes of chapter 273, be the custodian of resources and equipment located in and operated, supported, and managed by the state data center.

(f) Assume administrative access rights to resources and equipment, including servers, network components, and other devices, consolidated into the state data center.

1. Upon consolidation, a state agency shall relinquish administrative rights to consolidated resources and equipment. State agencies required to comply with federal and state criminal justice information security rules and policies shall retain administrative access rights sufficient to comply with the management control provisions of those rules and policies; however, the state data center shall have the appropriate type or level of rights to allow the center to comply with its duties pursuant to this section. The Department of Law Enforcement shall serve as the arbiter of disputes pertaining to the appropriate type and level of administrative access rights pertaining to the provision of management control in accordance with the federal criminal justice information guidelines.

2. The state data center shall provide customer entities with access to applications, servers, network components, and other devices necessary for entities to perform business activities and functions, and as defined and documented in a service-level agreement.

(g) In its procurement process, show preference for cloud-

492 computing solutions that minimize or do not require the
493 purchasing, financing, or leasing of state data center
494 infrastructure, and that meet the needs of customer agencies,
495 that reduce costs, and that meet or exceed the applicable state
496 and federal laws, regulations, and standards for cybersecurity.
497 (h) Assist customer entities in transitioning from state
498 data center services to the Northwest Regional Data Center or
499 other third-party cloud-computing services procured by a
500 customer entity or by the Northwest Regional Data Center on
501 behalf of a customer entity.
502 (2) USE OF THE STATE DATA CENTER.—The following are exempt
503 from the use of the state data center: the Department of Law
504 Enforcement, the Department of the Lottery's Gaming System,
505 Systems Design and Development in the Office of Policy and
506 Budget, the regional traffic management centers as described in
507 s. 335.14(2) and the Office of Toll Operations of the Department
508 of Transportation, the State Board of Administration, state
509 attorneys, public defenders, criminal conflict and civil
510 regional counsel, capital collateral regional counsel, and the
511 Florida Housing Finance Corporation.
512 (3) AGENCY LIMITATIONS.—Unless exempt from the use of the
513 state data center pursuant to this section or authorized by the
514 Legislature, a state agency may not:
515 (a) Create a new agency computing facility or data center,
516 or expand the capability to support additional computer

equipment in an existing agency computing facility or data center; or

(b) Terminate services with the state data center without giving written notice of intent to terminate services 180 days before such termination.

(4) DEPARTMENT RESPONSIBILITIES.—The department shall provide operational management and oversight of the state data center, which includes:

(a) Implementing industry standards and best practices for the state data center's facilities, operations, maintenance, planning, and management processes.

(b) Developing and implementing cost-recovery mechanisms that recover the full direct and indirect cost of services through charges to applicable customer entities. Such cost-recovery mechanisms must comply with applicable state and federal regulations concerning distribution and use of funds and must ensure that, for any fiscal year, no service or customer entity subsidizes another service or customer entity. The department may recommend other payment mechanisms to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives. Such mechanisms may be implemented only if specifically authorized by the Legislature.

(c) Developing and implementing appropriate operating guidelines and procedures necessary for the state data center to

perform its duties pursuant to subsection (1). The guidelines and procedures must comply with applicable state and federal laws, regulations, and policies and conform to generally accepted governmental accounting and auditing standards. The guidelines and procedures must include, but need not be limited to:

1. Implementing a consolidated administrative support structure responsible for providing financial management, procurement, transactions involving real or personal property, human resources, and operational support.

2. Implementing an annual reconciliation process to ensure that each customer entity is paying for the full direct and indirect cost of each service as determined by the customer entity's use of each service.

3. Providing rebates that may be credited against future billings to customer entities when revenues exceed costs.

4. Requiring customer entities to validate that sufficient funds exist before implementation of a customer entity's request for a change in the type or level of service provided, if such change results in a net increase to the customer entity's cost for that fiscal year.

5. By November 15 of each year, providing to the Office of Policy and Budget in the Executive Office of the Governor and to the chairs of the legislative appropriations committees the projected costs of providing data center services for the

following fiscal year.

6. Providing a plan for consideration by the Legislative Budget Commission if the cost of a service is increased for a reason other than a customer entity's request made pursuant to subparagraph 4. Such a plan is required only if the service cost increase results in a net increase to a customer entity for that fiscal year.

7. Standardizing and consolidating procurement and contracting practices.

(d) In collaboration with the Department of Law Enforcement and the Florida Digital Service, developing and implementing a process for detecting, reporting, and responding to cybersecurity incidents, breaches, and threats.

(e) Adopting rules relating to the operation of the state data center, including, but not limited to, budgeting and accounting procedures, cost-recovery methodologies, and operating procedures.

(5) NORTHWEST REGIONAL DATA CENTER CONTRACT.—In order for the department to carry out its duties and responsibilities relating to the state data center, the state chief information officer shall assume responsibility for the contract entered into by the secretary of the department ~~shall contract by July 1, 2022,~~ with the Northwest Regional Data Center pursuant to s. 287.057(11). The contract shall provide that the Northwest Regional Data Center will manage the operations of the state

data center and provide data center services to state agencies. Notwithstanding the terms of the contract, the Northwest Regional Data Center must provide the Florida Digital Service with access to information regarding the operations of the state data center.

(a) The department shall provide contract oversight, including, but not limited to, reviewing invoices provided by the Northwest Regional Data Center for services provided to state agency customers.

(b) The department shall approve or request updates to invoices within 10 business days after receipt. If the department does not respond to the Northwest Regional Data Center, the invoice will be approved by default. The Northwest Regional Data Center must submit approved invoices directly to state agency customers.

(6) FLORIDA DIGITAL SERVICE ACCESS.—The state data center, and any successor entity assuming the responsibilities of the state data center including, but not limited to, the Northwest Regional Data Center, shall provide the Florida Digital Service with full access to any infrastructure, system, application, or other means that hosts, supports, or manages data in the custody of an enterprise. For any such infrastructure, system, application, or other means, the state data center or a successor entity shall fully integrate with the Cybersecurity Operations Center.

(7) STATE DATA CENTER REPORT.—Subject to s. 119.0725, the state data center and any successor entity must submit to the department and the Florida Digital Service a quarterly report that provides, relating to infrastructure servicing enterprise customers and data, the number of:

(a) Technology assets which are within 1 year of end of life as defined by the manufacturer.

(b) Technology assets which are beyond end of life as defined by the manufacturer.

(c) Technology assets which are within 2 years of being unsupported by the manufacturer.

(d) Technology assets which are currently unsupported by the manufacturer.

(e) Workloads which are hosted by a commercial cloud service provider as defined in the National Institute of Standards and Technology, publication 500-292.

(f) Workloads which are not hosted by a commercial entity which is a cloud service provider as defined in the National Institute of Standards and Technology, publication 500-292.

(g) Service level disruptions and average duration of disruption.

Section 6. Subsection (10) of section 282.318, Florida Statutes, is renumbered as subsection (11), subsections (3) and (4) are amended, and a new subsection (10) is added to that section, to read:

282.318 Cybersecurity.—

(3) The department, 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. Such standards and processes must be consistent with generally accepted technology best practices, including the National Institute for Standards and Technology Cybersecurity Framework, for cybersecurity. The department, acting through the Florida Digital Service, shall adopt rules that mitigate risks; safeguard state agency digital assets, data, information, and information technology resources to ensure availability, confidentiality, and integrity; and support a security governance framework. The department, acting through the Florida Digital Service, shall also:

(a) Designate an employee of the Florida Digital Service as the state chief information security officer. The state chief information security officer must have experience and expertise in security and risk management for communications and information technology resources. The state chief information security officer is responsible for the development, operation, and oversight of cybersecurity for state technology systems. The state chief information security officer shall be notified of all confirmed or suspected incidents or threats of state agency information technology resources and must report such incidents

or threats to the state chief information officer and the Governor.

(b) Develop, and annually update by February 1, a statewide cybersecurity strategic plan that includes security goals and objectives for cybersecurity, including the identification and mitigation of risk, proactive protections against threats, tactical risk detection, threat reporting, and response and recovery protocols for a cyber incident.

(c) Develop and publish for use by state agencies a cybersecurity governance framework that, at a minimum, includes guidelines and processes for:

1. Establishing asset management procedures to ensure that an agency's information technology resources are identified and managed consistent with their relative importance to the agency's business objectives.

2. Using a standard risk assessment methodology that includes the identification of an agency's priorities, constraints, risk tolerances, and assumptions necessary to support operational risk decisions.

3. Completing comprehensive risk assessments and cybersecurity audits, which may be completed by a private sector vendor, and submitting completed assessments and audits to the department.

4. Identifying protection procedures to manage the protection of an agency's information, data, and information

technology resources.

5. Establishing procedures for accessing information and data to ensure the confidentiality, integrity, and availability of such information and data.

6. Detecting threats through proactive monitoring of events, continuous security monitoring, and defined detection processes.

7. Establishing agency cybersecurity incident response teams and describing their responsibilities for responding to cybersecurity incidents, including breaches of personal information containing confidential or exempt data.

8. Recovering information and data in response to a cybersecurity incident. The recovery may include recommended improvements to the agency processes, policies, or guidelines.

9. Establishing a cybersecurity incident reporting process that includes procedures for notifying the department and the Department of Law Enforcement of cybersecurity incidents.

a. The level of severity of the cybersecurity incident is defined by the National Cyber Incident Response Plan of the United States Department of Homeland Security as follows:

(I) Level 5 is an emergency-level incident within the specified jurisdiction that poses an imminent threat to the provision of wide-scale critical infrastructure services; national, state, or local government security; or the lives of the country's, state's, or local government's residents.

(II) Level 4 is a severe-level incident that is likely to result in a significant impact in the affected jurisdiction to public health or safety; national, state, or local security; economic security; or civil liberties.

(III) Level 3 is a high-level incident that is likely to result in a demonstrable impact in the affected jurisdiction to public health or safety; national, state, or local security; economic security; civil liberties; or public confidence.

(IV) Level 2 is a medium-level incident that may impact public health or safety; national, state, or local security; economic security; civil liberties; or public confidence.

(V) Level 1 is a low-level incident that is unlikely to impact public health or safety; national, state, or local security; economic security; civil liberties; or public confidence.

b. The cybersecurity incident reporting process must specify the information that must be reported by a state agency following a cybersecurity incident or ransomware incident, which, at a minimum, must include the following:

(I) A summary of the facts surrounding the cybersecurity incident or ransomware incident.

(II) The date on which the state agency most recently backed up its data; the physical location of the backup, if the backup was affected; and if the backup was created using cloud computing.

(III) The types of data compromised by the cybersecurity incident or ransomware incident.

(IV) The estimated fiscal impact of the cybersecurity incident or ransomware incident.

(V) In the case of a ransomware incident, the details of the ransom demanded.

c.(I) A state agency shall report all ransomware incidents and ~~any~~ cybersecurity incidents ~~incident determined by the state agency to be of severity level 3, 4, or 5~~ to the Florida Digital Service, the Cybersecurity Operations Center, and the Cybercrime Office of the Department of Law Enforcement as soon as possible but no later than 4 ~~48~~ hours after discovery of the cybersecurity incident and no later than 2 ~~12~~ hours after discovery of the ransomware incident. The report must contain the information required in sub-subparagraph b. The Florida Digital Service shall notify the Governor, the President of the Senate, and the Speaker of the House of Representatives of any incident discovered by a state agency but not timely reported under this sub-sub-subparagraph.

(II) The Cybersecurity Operations Center shall notify the President of the Senate and the Speaker of the House of Representatives of any severity level 3, 4, or 5 incident as soon as possible but no later than 12 hours after receiving a state agency's incident report. The notification must include a high-level description of the incident and the likely effects

and must be provided in a secure environment.

d. ~~A state agency shall report a cybersecurity incident determined by the state agency to be of severity level 1 or 2 to the Cybersecurity Operations Center and the Cybercrime Office of the Department of Law Enforcement as soon as possible. The report must contain the information required in sub-subparagraph b.~~

~~c.~~ The Cybersecurity Operations Center shall provide a consolidated incident report by the 15th day after the end of each quarter ~~on a quarterly basis~~ to the President of the Senate, the Speaker of the House of Representatives, and the Florida Cybersecurity Advisory Council. The report provided to the Florida Cybersecurity Advisory Council may not contain the name of any agency, network information, or system identifying information but must contain sufficient relevant information to allow the Florida Cybersecurity Advisory Council to fulfill its responsibilities as required in s. 282.319(9).

10. Incorporating information obtained through detection and response activities into the agency's cybersecurity incident response plans.

11. Developing agency strategic and operational cybersecurity plans required pursuant to this section.

12. Establishing the managerial, operational, and technical safeguards for protecting state government data and information technology resources that align with the state

agency risk management strategy and that protect the confidentiality, integrity, and availability of information and data.

13. Establishing procedures for procuring information technology commodities and services that require the commodity or service to meet the National Institute of Standards and Technology Cybersecurity Framework.

14. Submitting after-action reports following a cybersecurity incident or ransomware incident. Such guidelines and processes for submitting after-action reports must be developed and published by December 1, 2022.

(d) Assist state agencies in complying with this section.

(e) In collaboration with the Cybercrime Office of the Department of Law Enforcement, annually provide training for state agency information security managers and computer security incident response team members that contains training on cybersecurity, including cybersecurity threats, trends, and best practices.

(f) Annually review the strategic and operational cybersecurity plans of state agencies.

(g) Annually provide cybersecurity training to all state agency technology professionals and employees with access to highly sensitive information which develops, assesses, and documents competencies by role and skill level. The cybersecurity training curriculum must include training on the

identification of each cybersecurity incident severity level referenced in sub-subparagraph (c)9.a. The training may be provided in collaboration with the Cybercrime Office of the Department of Law Enforcement, a private sector entity, or an institution of the State University System.

(h) Operate and maintain a Cybersecurity Operations Center led by the state chief information security officer, which must be primarily virtual and staffed with tactical detection and incident response personnel. The Cybersecurity Operations Center shall serve as a clearinghouse for threat information and coordinate with the Department of Law Enforcement to support state agencies and their response to any confirmed or suspected cybersecurity incident.

(i) Lead an Emergency Support Function, ESF CYBER and DIGITAL, under the state comprehensive emergency management plan as described in s. 252.35.

(j) Provide cybersecurity briefings to the members of any legislative committee or subcommittee responsible for policy matters relating to cybersecurity.

(k) Have the authority to respond to any state agency cybersecurity incident.

(4) Each state agency head shall, at a minimum:

(a) Designate a chief information security officer to integrate the agency's technical and operational cybersecurity efforts with the Cybersecurity Operations Center. This

designation must be provided annually in writing to the Florida Digital Service by January 1. An agency's chief information security officer shall report to the agency's chief information officer. An agency may request the department to procure a chief information security officer as a service to fulfill the agency's duties under this paragraph.

(b) ~~(a)~~ Designate an information security manager to ensure compliance with cybersecurity governance, manage risk, and ensure compliance with the state's incident response plan ~~administer the cybersecurity program of the state agency~~. This designation must be provided annually in writing to the department by January 15 ~~1~~. A state agency's information security manager, for purposes of these information security duties, shall report directly to the agency head.

(c) ~~(b)~~ In consultation with the department, through the Florida Digital Service, and the Cybercrime Office of the Department of Law Enforcement, and incorporating the resources of the Florida State Guard as appropriate, establish an agency cybersecurity response team to respond to a cybersecurity incident. The agency cybersecurity response team shall convene upon notification of a cybersecurity incident and must immediately report all confirmed or suspected incidents to the state chief information security officer, or his or her designee, and comply with all applicable guidelines and processes established pursuant to paragraph (3)(c).

(d) ~~(c)~~ Submit to the department annually by July 31, the state agency's strategic and operational cybersecurity plans developed pursuant to rules and guidelines established by the department, through the Florida Digital Service.

1. The state agency strategic cybersecurity plan must cover a 3-year period and, at a minimum, define security goals, intermediate objectives, and projected agency costs for the strategic issues of agency information security policy, risk management, security training, security incident response, and disaster recovery. The plan must be based on the statewide cybersecurity strategic plan created by the department and include performance metrics that can be objectively measured to reflect the status of the state agency's progress in meeting security goals and objectives identified in the agency's strategic information security plan.

2. The state agency operational cybersecurity plan must include a progress report that objectively measures progress made towards the prior operational cybersecurity plan and a project plan that includes activities, timelines, and deliverables for security objectives that the state agency will implement during the current fiscal year.

(e) ~~(d)~~ Conduct, and update annually by April 30 ~~every 3 years~~, a comprehensive risk assessment, which may be facilitated by the department or completed by a private sector vendor, to determine the security threats to the data, information, and

information technology resources, including mobile devices and print environments, of the agency. The risk assessment must comply with the risk assessment criteria, methodology, and scope developed by the state chief information security officer. The risk assessment findings must be signed by the agency head or the agency head's designee and the Florida Digital Service. The risk assessment ~~methodology developed by the department and~~ is confidential and exempt from s. 119.07(1), except that such information shall be available to the Auditor General, the Florida Digital Service within the department, the Cybercrime Office of the Department of Law Enforcement, and, for state agencies under the jurisdiction of the Governor, the Chief Inspector General. If a private sector vendor is used to complete a comprehensive risk assessment, it must attest to the validity of the risk assessment findings.

(f) ~~(e)~~ Develop, and periodically update, written internal policies and procedures, which include procedures for reporting cybersecurity incidents and breaches to the Cybercrime Office of the Department of Law Enforcement and the Florida Digital Service within the department. Such policies and procedures must be consistent with the rules, guidelines, and processes established by the department to ensure the security of the data, information, and information technology resources of the agency. The internal policies and procedures that, if disclosed, could facilitate the unauthorized modification, disclosure, or

destruction of data or information technology resources are confidential information and exempt from s. 119.07(1), except that such information shall be available to the Auditor General, the Cybercrime Office of the Department of Law Enforcement, the Florida Digital Service within the department, and, for state agencies under the jurisdiction of the Governor, the Chief Inspector General.

(g) ~~(f)~~ Implement managerial, operational, and technical safeguards and risk assessment remediation plans recommended by the department to address identified risks to the data, information, and information technology resources of the agency. The department, through the Florida Digital Service, shall track implementation by state agencies upon development of such remediation plans in coordination with agency inspectors general.

(h) ~~(g)~~ Ensure that periodic internal audits and evaluations of the agency's cybersecurity program for the data, information, and information technology resources of the agency are conducted. The results of such audits and evaluations are confidential information and exempt from s. 119.07(1), except that such information shall be available to the Auditor General, the Cybercrime Office of the Department of Law Enforcement, the Florida Digital Service within the department, and, for agencies under the jurisdiction of the Governor, the Chief Inspector General.

(i) ~~(h)~~ Ensure that the cybersecurity requirements in the written specifications for the solicitation, contracts, and service-level agreement of information technology and information technology resources and services meet or exceed the applicable state and federal laws, regulations, and standards for cybersecurity, including the National Institute of Standards and Technology Cybersecurity Framework. Service-level agreements must identify service provider and state agency responsibilities for privacy and security, protection of government data, personnel background screening, and security deliverables with associated frequencies.

(j) ~~(i)~~ Provide cybersecurity awareness training to all state agency employees within 30 days after commencing employment, and annually thereafter, concerning cybersecurity risks and the responsibility of employees to comply with policies, standards, guidelines, and operating procedures adopted by the state agency to reduce those risks. The training may be provided in collaboration with the Cybercrime Office of the Department of Law Enforcement, a private sector entity, or an institution of the State University System.

(k) ~~(j)~~ Develop a process for detecting, reporting, and responding to threats, breaches, or cybersecurity incidents which is consistent with the security rules, guidelines, and processes established by the department through the Florida Digital Service.

1. All cybersecurity incidents and ransomware incidents must be reported by state agencies. Such reports must comply with the notification procedures and reporting timeframes established pursuant to paragraph (3)(c).

2. For cybersecurity breaches, state agencies shall provide notice in accordance with s. 501.171.

(l) ~~(k)~~ Submit to the Florida Digital Service, within 1 week after the remediation of a cybersecurity incident or ransomware incident, an after-action report that summarizes the incident, the incident's resolution, and any insights gained as a result of the incident.

(10) Any legislative committee or subcommittee responsible for policy matters relating to cybersecurity may hold meetings closed by the respective legislative body under the rules of such legislative body at which such committee or subcommittee is briefed on records made confidential and exempt under subsections (5) and (6). The committee or subcommittee must maintain the confidential and exempt status of such records.

Section 7. Paragraph (d) of subsection (5) of section 282.3185, Florida Statutes, is redesignated as paragraph (c), and paragraph (b) and present paragraph (c) of that subsection are amended to read:

282.3185 Local government cybersecurity.—

(5) INCIDENT NOTIFICATION.—

(b)1. A local government shall report all ransomware

incidents and ~~any~~ cybersecurity incidents ~~incident determined by the local government to be of severity level 3, 4, or 5~~ as provided in s. 282.318(3)(c) to the Florida Digital Service, the Cybersecurity Operations Center, the Cybercrime Office of the Department of Law Enforcement, and the sheriff who has jurisdiction over the local government as soon as possible but no later than 4 ~~48~~ hours after discovery of the cybersecurity incident and no later than 2 ~~12~~ hours after discovery of the ransomware incident. The report must contain the information required in paragraph (a). The Florida Digital Service shall notify the Governor, the President of the Senate, and the Speaker of the House of Representatives of any incident discovered by a local government but not timely reported under this subparagraph.

2. The Cybersecurity Operations Center shall notify the President of the Senate and the Speaker of the House of Representatives of any severity level 3, 4, or 5 incident as soon as possible but no later than 12 hours after receiving a local government's incident report. The notification must include a high-level description of the incident and the likely effects and must be provided in a secure environment.

~~(c) A local government may report a cybersecurity incident determined by the local government to be of severity level 1 or 2 as provided in s. 282.318(3)(c) to the Cybersecurity Operations Center, the Cybercrime Office of the Department of~~

~~Law Enforcement, and the sheriff who has jurisdiction over the local government. The report shall contain the information required in paragraph (a).~~

Section 8. Paragraph (j) of subsection (4) of section 282.319, Florida Statutes, is amended to read:

282.319 Florida Cybersecurity Advisory Council.—

(4) The council shall be comprised of the following members:

(j) Three representatives from critical infrastructure sectors, ~~one of whom must be from a water treatment facility,~~ appointed by the Governor.

Section 9. Section 768.401, Florida Statutes, is created to read:

768.401 Limitation on liability for cybersecurity incidents.—

(1) A county or municipality that substantially complies with s. 282.3185 shall not be liable in connection with a cybersecurity incident.

(2) A sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information shall not be liable in connection with a cybersecurity incident if the entity substantially complies with s. 501.171, if applicable, and has:

(a) Adopted a cybersecurity program that substantially

aligns with the current version of any of the following standards:

1. The National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity.

2. NIST special publication 800-171.

3. NIST special publications 800-53 and 800-53A.

4. The Federal Risk and Authorization Management Program security assessment framework.

5. CIS Critical Security Controls.

6. The International Organization for Standardization/International Electrotechnical Commission 27000-series family of standards; or

(b) If regulated by the state or Federal Government, or both, or if otherwise subject to the requirements of any of the following laws and regulations, substantially complied its cybersecurity program to the current version of the following, as applicable:

1. The security requirements of the Health Insurance Portability and Accountability Act of 1996, 45 C.F.R. part 164 subpart C.

2. Title V of the Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, as amended.

3. The Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283.

4. The Health Information Technology for Economic and Clinical Health Act, 45 C.F.R. part 162.

(c) The scale and scope of compliance with a program or standard under paragraphs (a) or (b) by a covered entity, as applicable, is appropriate if it is based on all of the following factors:

1. The size and complexity of the covered entity;

2. The nature and scope of the activities of the covered entity; and

3. The sensitivity of the information to be protected.

(3) Any commercial entity covered by subsection (2) that substantially complies with a combination of industry-recognized cybersecurity frameworks or standards, including the payment card industry data security standard, to gain the presumption against liability pursuant to subsection (2) must, upon the revision of two or more of the frameworks or standards with which the entity complies, adopt the revised frameworks or standards within 1 year after the latest publication date stated in the revisions.

(4) This section does not establish a private cause of action. Failure of a county, municipality, or commercial entity to substantially implement a cybersecurity program that is in compliance with this section is not evidence of negligence and does not constitute negligence per se.

(5) In an action in connection with a cybersecurity

incident, if the defendant is an entity covered by subsections (1) or (2), the defendant has the burden of proof to establish substantial compliance.

Section 10. This act shall take effect July 1, 2023.

---

**T I T L E A M E N D M E N T**

Remove everything before the enacting clause and insert:

A bill to be entitled

An act relating to cybersecurity; providing a short title; amending s. 110.205, F.S.; exempting certain personnel from the career service; amending s. 282.0041, F.S.; providing and revising definitions; amending s. 282.0051, F.S.; requiring the Florida Digital Service to ensure that independent project oversight is performed in a certain manner and take certain actions relating to the procurement of project oversight as a service; requiring the Florida Digital Service to provide certain reports by certain dates; requiring the Florida Digital Service to establish an operations committee for a certain purpose and composed of certain members; requiring the Governor to appoint a state chief information officer subject to confirmation by the Senate; requiring the state chief information officer to designate a state chief

technology officer; amending s. 282.201, F.S.; providing that the state data center shall be overseen by and accountable to the Department of Management Services in consultation with certain officers; providing requirements for certain state data center procurements; requiring the Florida Digital Service to be provided with full access to state data center infrastructure, systems, applications, and other means of hosting, supporting, and managing certain data; requiring the state data center to submit a certain report to the department and the Florida Digital Service; amending s. 282.318, F.S.; requiring a state agency to report ransomware and cybersecurity incidents within a certain time period; requiring the Florida Digital Service to notify the Governor and Legislature of certain incidents; providing that certain notification must be provided in a secure environment; requiring the Florida Digital Service to provide cybersecurity briefings to certain legislative committees; authorizing the Florida Digital Service to respond to certain cybersecurity incidents; requiring a state agency head to designate a chief information security officer for the agency; revising the purpose of an agency's information security manager; revising the frequency of a comprehensive risk assessment;

authorizing certain legislative committees to hold closed meetings to receive certain briefings; requiring such committees to maintain the confidential and exempt status of certain records; amending s. 282.3185, F.S.; requiring a local government to report ransomware and cybersecurity incidents within a certain time period; requiring the Florida Digital Service to notify the Governor and Legislature of certain incidents; providing that certain notification must be provided in a secure environment; amending s. 282.319, F.S.; revising the membership of the Florida Cybersecurity Advisory Council; creating s. 768.401, F.S.; providing a presumption against liability in connection with a cybersecurity incident for a county, municipality, or commercial entity that complies with certain requirements; requiring certain entities to adopt certain revised frameworks or standards within a specified time period; providing that a private cause of action is not established; providing that certain failures are not evidence of negligence and do not constitute negligence per se; providing an effective date.

# HOUSE OF REPRESENTATIVES STAFF ANALYSIS

**BILL #:** PCS for HB 1025 Government Vehicles
**SPONSOR(S):** Energy, Communications & Cybersecurity Subcommittee
**TIED BILLS:** **IDEN./SIM. BILLS:** CS/CS/SB 284

| REFERENCE | ACTION | ANALYST | STAFF DIRECTOR or BUDGET/POLICY CHIEF |
|---|---|---|---|
| Orig. Comm.: Energy, Communications & Cybersecurity Subcommittee | | Walsh | Keating |

## SUMMARY ANALYSIS

Current law requires state agencies that wish to procure commodities or contractual services in excess of $35,000 to use a competitive solicitation process. A competitive solicitation is the process of requesting and receiving two or more sealed bids, proposals, or replies submitted by responsive vendors in accordance with the terms of a competitive process.

State agencies, in many circumstances, are required to take specified actions to promote energy efficiency and other environmental benefits when conducting public business. When procuring new vehicles, state agencies, state universities, community colleges, and local governments under a state purchasing plan must first define the intended purpose for the vehicle and determine which statutorily listed use class applies. Vehicles must be selected for the greatest fuel efficiency available for the determined class when fuel economy data is available.

Under the bill, any governmental entity that purchases under the state purchasing plan must select vehicles based on the lowest lifetime ownership costs, including costs for fuel, operations, and maintenance.

The bill strikes the requirement under current law that state agencies use ethanol and biodiesel fuel when available, and the bill removes the requirement that state agencies that administer central fueling operations for state-owned vehicles procure biofuels for fleet needs to the greatest extent practicable.

The bill requires DMS to make recommendations before July 1, 2024, to state agencies and local governments regarding the procurement of electric vehicles and natural gas fuel vehicles.

The bill has no impact state or local government revenues or expenditures.

The bill provides an effective date of July 1, 2023.

## FULL ANALYSIS

## I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

**Present Situation**

Procurement of Commodities or Contractual Services

Current law specifies the procedures for procurement of commodities or contractual services.[1] The Department of Management Services (DMS) provides uniform commodity and contractual service procurement policies, rules, procedures, and forms for use by agencies and eligible users,[2] and establishes purchasing agreements and procures state term contracts for commodities and contractual services.[3]

DMS is required to consider the life-cycle cost of commodities purchased by the state, when applicable and feasible.[4] When calculating the life-cycle cost, the agency may consider the acquisition cost of the product; the energy consumption and the projected cost of energy over the useful life of the product; and the anticipated trade-in, resale, or salvage value of the product.[5] The agency is authorized to establish by rule energy-efficiency standards for major energy-consuming products.[6]

Florida law requires state agencies that wish to procure commodities or contractual services in excess of $35,000[7] to use a competitive solicitation process.[8] Competitive solicitation is the process of requesting and receiving two or more sealed bids, proposals, or replies submitted by responsive vendors in accordance with the terms of a competitive process, regardless of procurement method.[9]

Commodities or contractual services available only from a single source may be exempt from the competitive solicitation requirement.[10] Current law specifies the processes an agency must follow in this circumstance.[11]

Climate-friendly Public Business

Current law requires state agencies, in many circumstances, to take specified actions to promote energy efficiency and other environmental benefits when conducting public business.[12] These actions include:

- Consulting the Florida Climate-Friendly Preferred Products List[13] when procuring products from state term contracts[14] and procuring such products if the price is comparable;[15]
- Contracting for meeting and conference space only with facilities that have received a special designation from the Department of Environmental Protection for best practices in water,

[1] Ch. 287, F.S.
[2] S. 287.032, F.S.
[3] S. 287.042(2)(a), F.S.
[4] S. 287.083(1), F.S.
[5] S. 287.083(5), F.S.
[6] S. 287.083(3)(a), F.S.
[7] S. 287.017(2), F.S.
[8] S. 287.057(1), F.S.
[9] S. 287.012(6), F.S.
[10] S. 287.057(3)(c), F.S.
[11] *Id.*
[12] S. 286.29, F.S.
[13] The Florida Climate-Friendly Preferred Products List is developed by DMS, which works with the Department of Environmental Protection to continually assess the list. The list identifies specific products and vendors that offer energy efficiency or other environmental benefits over competing products. *See* s. 286.29(1), F.S.
[14] A state term contract is a contract for commodities or contractual services that is competitively procured by DMS and is used by agencies and other eligible users. *See* ss. 287.012(28), F.S. and 287.042(2)(a), F.S.
[15] S. 286.29(1), F.S.

energy, and waste efficiency standards, absent a determination from the agency head no other viable alternative exists;[16]
- Ensuring all maintained vehicles meet minimum maintenance schedules shown to reduce fuel consumption and reporting compliance to DMS;[17] and
- Using ethanol and biodiesel blended fuels when available. State agencies administering central fueling operations for state-owned vehicles shall procure biofuels for fleet needs to the greatest extent practicable.[18]

Additionally, state agencies, state universities, community colleges, and local governments that purchase vehicles under a state purchasing plan must first define the intended purpose for the vehicle and determine which statutorily listed use class[19] the vehicle is being procured for.[20] These vehicles must be selected for the greatest fuel efficiency available for the determined use class when fuel economy data is available.[21] Exceptions may be made for emergency response vehicles in certain circumstances.[22]

**Effect of the Bill**

The bill requires any governmental entity that purchases under the state purchasing plan to select vehicles for each use class based on the lowest lifetime ownership costs, including costs for fuel, operations, and maintenance, rather than based on the greatest fuel efficiency.

The bill strikes the requirement under current law that state agencies use ethanol and biodiesel fuel when available. It also removes the requirement that state agencies that administer central fueling operations for state-owned vehicles procure biofuels for fleet needs to the greatest extent practicable.

The bill requires DMS to make recommendations before July 1, 2024, to state agencies, state colleges and universities, and local governments regarding the procurement of electric vehicles and natural gas fuel vehicles and the best practices for integrating those vehicles into existing fleets.

The bill provides an effective date of July 1, 2023.

B. SECTION DIRECTORY:

**Section 1:** Amends s. 286.29, F.S., relating to climate-friendly public business.

**Section 2:** Requires DMS to make specified recommendations.

**Section 3:** Provides an effective date of July 1, 2023.

## II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

None.

[16] S. 286.29(2), F.S.
[17] S. 286.29(3), F.S.
[18] S. 286.29(5), F.S.
[19] Listed vehicle use classes are the following: state business travel, designated operator; state business travel, pool operators; construction, agricultural, or maintenance work; conveyance of passengers; conveyance of building or maintenance materials and supplies; off-road vehicle, motorcycle, or all-terrain vehicle; emergency response; or other. *See* s. 286.29(4), F.S.
[20] S. 286.29(4), F.S.
[21] *Id.*
[22] *Id.*

2. Expenditures:

None.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

None.

2. Expenditures:

None.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

None.

D. FISCAL COMMENTS:

None.

## III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

Not applicable. This bill does not appear to require counties or municipalities to spend funds or take action requiring the expenditures of funds; reduce the authority that counties or municipalities have to raise revenues in the aggregate; or reduce the percentage of state tax shared with counties or municipalities.

2. Other:

None.

B. RULE-MAKING AUTHORITY:

None.

C. DRAFTING ISSUES OR OTHER COMMENTS:

None.

## IV. AMENDMENTS/COMMITTEE SUBSTITUTE CHANGES

A bill to be entitled

An act relating to government vehicles; amending s. 286.29, F.S.; revising the selection criteria for purchasing or leasing vehicles for state agencies, state universities, community colleges, and local governments under a state purchasing plan; deleting a provision requiring the use and procurement of ethanol and biodiesel blended fuels; requiring the Department of Management Services, before a specified date, to make recommendations to state agencies, state universities, community colleges, and local governments relating to the procurement and integration of electric and natural gas fuel vehicles; providing an effective date.

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

Section 1. Subsections (4) and (5) of section 286.29, Florida Statutes, are amended to read:

286.29 Climate-friendly public business.—The Legislature recognizes the importance of leadership by state government in the area of energy efficiency and in reducing the greenhouse gas emissions of state government operations. The following shall pertain to all state agencies when conducting public business:

(4) When procuring new vehicles, all state agencies, state



CODING: Words stricken are deletions; words underlined are additions.

universities, community colleges, and local governments that purchase vehicles under a state purchasing plan shall first define the intended purpose for the vehicle and determine which of the following use classes for which the vehicle is being procured:

(a) State business travel, designated operator;

(b) State business travel, pool operators;

(c) Construction, agricultural, or maintenance work;

(d) Conveyance of passengers;

(e) Conveyance of building or maintenance materials and supplies;

(f) Off-road vehicle, motorcycle, or all-terrain vehicle;

(g) Emergency response; or

(h) Other.

Vehicles described in paragraphs (a) through (h), when being processed for purchase or leasing agreements, must be selected based on the lowest lifetime ownership costs, including costs for fuel, operations, and maintenance, ~~for the greatest fuel efficiency available~~ for a given use class ~~when fuel economy data are available~~. Exceptions may be made for individual vehicles in paragraph (g) when accompanied, during the procurement process, by documentation indicating that the operator or operators will exclusively be emergency first responders or have special documented need for exceptional



CODING: Words ~~stricken~~ are deletions; words underlined are additions.

vehicle performance characteristics. Any request for an exception must be approved by the purchasing agency head and any exceptional performance characteristics denoted as a part of the procurement process prior to purchase.

~~(5) All state agencies shall use ethanol and biodiesel blended fuels when available. State agencies administering central fueling operations for state-owned vehicles shall procure biofuels for fleet needs to the greatest extent practicable.~~

Section 2. Before July 1, 2024, the Department of Management Services shall make recommendations to state agencies, state universities, community colleges, and local governments regarding the procurement of electric and natural gas fuel vehicles and best practices for integrating such vehicles into existing fleets.

Section 3. This act shall take effect July 1, 2023.



CODING: Words ~~stricken~~ are deletions; words underlined are additions.

**PCS for HB 1331**

# HOUSE OF REPRESENTATIVES STAFF ANALYSIS

**BILL #:** PCS for HB 1331 Municipal Utilities
**SPONSOR(S):** Energy, Communications & Cybersecurity Subcommittee
**TIED BILLS:** **IDEN./SIM. BILLS:**

| REFERENCE | ACTION | ANALYST | STAFF DIRECTOR or BUDGET/POLICY CHIEF |
|---|---|---|---|
| Orig. Comm.: Energy, Communications & Cybersecurity Subcommittee | | Walsh | Keating |

## SUMMARY ANALYSIS

Pursuant to s. 2(b), Art. VIII of the State Constitution, municipalities have the governmental, corporate, and proprietary powers to enable them to conduct municipal government, perform municipal functions, and render municipal services. Under their home rule power and as otherwise provided or limited by law or agreement, municipalities may provide utilities to citizens and entities within the municipality's corporate boundaries, in unincorporated areas, and even in other municipalities.

Many municipalities own and operate electric utilities and natural gas utilities and govern the operation of those utilities through ordinance, code, or policies. Municipalities are also authorized by general law to provide water and sewer utility services. A municipality that operates a water or sewer utility outside of its municipal boundaries may impose higher rates, fees, and charges on consumers receiving service outside of its corporate boundaries as compared to the rates, fees, and charges imposed on consumers within its boundaries. Municipalities routinely transfer a portion of their utility earnings to their general funds for non-utility purposes, though the amounts and percentages may vary widely among municipalities.

The bill places limits on the portion of municipal utility revenues that may be used to fund or finance a municipality's non-utility related general government functions. In doing so, the bill limits the rate of transfer for municipal electric, natural gas, and water or wastewater utilities. Under the bill, the greater the proportion of customers outside of the city boundaries that a municipal utility serves, the lower the cap is on transfers. However, if a municipal utility is governed by a utility authority board that, through the election of voting members from outside the municipal boundaries, provides for representation of retail customers located outside the municipal boundaries approximately proportionate to the percentage of such customers, then transfers of revenue are not subject to a reduced cap.

The bill removes a provision allowing water or sewer utilities to add, for consumers outside of its boundaries, a surcharge of up to 25 percent of the rates, fees, and charges imposed on consumers within its boundaries. Furthermore, the bill changes the limit on the rates, fees, and charges such utility can impose on customers outside of municipal boundaries to no more than 25 percent above the total amount the municipal water or sewer utility charges customers within the municipal boundaries, provided rates for outside customers are set in a public hearing using the same methods as rates for other customers.

The bill limits the rates, fees, and charges that a municipal water or sewer utility that provides service to consumers within the boundaries of a separate municipality, using a water treatment plant or sewer treatment plant located within the boundaries of that separate municipality, by requiring that such charges are no more that the rates, fees, and charges imposed on consumers inside its own municipal boundaries.

The bill will not impact state government revenues and state or local government expenditures. The bill may have a negative fiscal impact on certain local revenues. *See* Fiscal Analysis & Economic Impact Statement.

The bill provides an effective date of July 1, 2024.

**This bill may be a county or municipality mandate requiring a two-thirds vote of the membership of the House. See Section III.A.1 of the analysis.**

## FULL ANALYSIS

## I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

**Present Situation**

Local Government Utility Services

Pursuant to s. 2(b), Art. VIII of the State Constitution, municipalities have the governmental, corporate, and proprietary powers to enable them to conduct municipal government, perform municipal functions, and render municipal services. Municipalities may exercise any power for municipal purposes, except when expressly prohibited by law.[1] The legislative body of each municipality has the power to enact legislation on any subject upon which the state Legislature may act with certain exceptions.[2] Under their home rule power and as otherwise provided or limited by law or agreement, municipalities may provide utilities to citizens and entities within the municipality's corporate boundaries, in unincorporated areas, and even in other municipalities.

Many municipalities own and operate electric utilities and natural gas utilities and govern the operation of those utilities through ordinance, code, or policies. Currently, there are 33 municipal electric utilities in the state.[3] Municipal electric and natural gas utility rates are not directly regulated by the Florida Public Service Commission (PSC), however, the PSC does have jurisdiction over municipal electric utilities for matters related to rate structure, power plant transmission line site certification, general reporting jurisdiction, service territory and territory disputes, energy efficiency reporting, ten year site plans, reporting on system hardening and resiliency, reporting on net metering, audits related to regulatory assessment fees, monitoring renewable energy, reporting on facilities inspection and vegetation management, and grid bill jurisdiction.[4]

Municipalities are authorized by general law to provide water and sewer utility services.[5] With respect to public works projects, including water and sewer utility services,[6] municipalities may extend and execute their corporate powers outside of their corporate limits as "desirable or necessary for the promotion of the public health, safety and welfare."[7] A municipality may not extend or apply these corporate powers within the corporate limits of another municipality.[8] However, it may permit any other municipality and the owners of lands outside its corporate limits or within the limits of another municipality to connect with its water and sewer utility facilities and use its services upon agreed terms and conditions.[9] An informal study conducted in 2014 indicated that approximately 250 municipalities provide water service and approximately 220 municipalities provide wastewater service. Of these municipalities, the study found that approximately 140 provide water and/or waste water services to

[1] Section 166.021(2), F.S., provides that any activity or power which may be exercised by the state or its political subdivisions is considered a municipal purpose.
[2] Pursuant to s. 166.021(3), F.S., a municipality may not enact legislation on the following: the subjects of annexation, merger, and exercise of extraterritorial power, which require general law or special law; any subject expressly prohibited by the constitution; any subject expressly preempted to state or county government by the constitution or by general law; and any subject preempted to a county pursuant to a county charter adopted under the authority of the State constitution.
[3] Presentation on *Florida Public Power*, Florida Municipal Electric Association (Feb. 9, 2023), slide 2, available at https://www.myfloridahouse.gov/Sections/Documents/loaddoc.aspx?PublicationType=Committees&CommitteeId=3226&Session=2023&DocumentType=Meeting+Packets&FileName=ecc+2-9-23.pdf.
[4] *Id.* at slide 3.
[5] Pursuant to s. 180.06, F.S., a municipality may "provide water and alternative water supplies;" "provide for the collection and disposal of sewage, including wastewater reuse, and other liquid wastes;" and "construct reservoirs, sewerage systems, trunk sewers, intercepting sewers, pumping stations, wells, siphons, intakes, pipelines, distribution systems, purification works, collection systems, treatment and disposal works" to accomplish these purposes.
[6] Other public works projects authorized under s. 180.06, F.S., include alternative water supplies, maintenance of water flow and bodies of water for sanitary purposes, garbage collection and disposal, airports, hospitals, jails, golf courses, gas plants and distribution systems, and related facilities.
[7] S. 180.02(2), F.S.
[8] *Id.*
[9] S. 180.19, F.S.

customers outside of their municipal boundaries, which may include customers in unincorporated areas of counties or in other municipalities.[10] These utility systems are exempt from PSC jurisdiction.

A municipality that operates a water or sewer utility outside of its municipal boundaries may impose higher rates, fees, and charges on consumers receiving service outside of its corporate boundaries as compared to the rates, fees, and charges imposed on consumers within its boundaries. The municipality can accomplish this in two ways:

- First, for consumers outside of its boundaries, it may add a surcharge of up to 25 percent of the rates, fees, and charges imposed on consumers within its boundaries. This mechanism does not require a public hearing.[11]
- Second, it may set separate rates, fees, and charges for consumers outside its boundaries based on the same factors used to set rates for consumers within its boundaries. It may add a surcharge of up to 25 percent of these charges, provided that the total of all such rates, fees, and charges for service to consumers outside its boundaries may not exceed the total charges to consumers within its boundaries by more than 50 percent for corresponding service. Rates set in this manner require a public hearing at which all users served or to be served by the water or sewer utilities and all other interested persons will have an opportunity to be heard concerning the proposed rates.[12]

There is no central repository for information concerning municipal water or sewer service rates that identifies municipalities that impose higher rates on consumers outside of the municipal boundaries, the specific mechanism used by such municipalities to establish such rates, or the level of any additional charge or surcharge imposed.

Most municipal utility systems are governed by the municipality's governing body (i.e., the city commission). Six municipal electric utility systems in Florida are governed by separate utility boards, or "authorities," which are typically appointed by the municipality's governing body.[13] These utility authorities vary in structure, though the charter documents for each generally address the powers and duties of the authority (including terms related to rate-setting, financing, acquisitions, and eminent domain), the selection process for authority members (including qualifications and terms of office), the management and personnel of the authority, the transfer of revenues from utility operations to the municipality, and the degree of continuing oversight by the municipal governing body.

Current law authorizes municipalities to raise amounts of money which are necessary for the conduct of the municipal government. A municipality may do so by taxation and licenses authorized by Florida's constitution or general law, or by user charges or fees authorized by ordinance.[14] Municipalities routinely transfer a portion of their utility earnings to their general funds for non-utility purposes, though the amounts and percentages may vary widely among municipalities.[15] These transfers may be limited in some circumstances by ordinance, but they are not governed by state law.

**Effect of the Bill**

The bill places limits on the portion of municipal utility revenues that may be used to fund or finance a municipality's non-utility related general government functions. In doing so, the bill limits the rate of transfer for municipal electric, natural gas, and water or wastewater utilities. Under the bill, the greater the proportion of customers outside of the city boundaries that a municipal utility serves, the lower the cap is on transfers.

[10] Analysis of House Bill 813 (2014), Florida House of Representatives.
[11] S. 180.191(1)(a), F.S.
[12] S. 180.191(1)(b), F.S.
[13] The Keys Energy Services Utility Board is the only utility authority in the state with elected board members. Key West has an elected board, with 2 of the 5 members from outside the city limits. Presentation on *Florida Public Power*, Florida Municipal Electric Association *supra* n. 6, slide 8.
[14] S. 166.201, F.S.
[15] Presentation on *Florida Public Power*, Florida Municipal Electric Association *supra* n. 6, slide 6.

Under the bill, revenues transferred to fund or finance non-utility governmental functions, which were generated by a municipal electric utility, may not exceed a rate equal to the amount derived by applying the average of the midpoints of the rates of return on equity approved by the PSC for each investor-owned electric utility in the state.

Similarly, the bill limits revenues transferred to fund or finance non-utility governmental functions, which were generated by a municipal natural gas utility by capping the transfer at a rate equal to the amount derived by applying the average of the midpoints of the rates of return on equity approved by the PSC for each investor-owned natural gas utility in the state.

Under the bill, revenues generated from a municipal water or wastewater utility may only be transferred at a rate equal to the amount derived by applying the rate of return on equity established by the PSC under s. 367.081(4)(f), F.S.[16]

The bill provides for reduction to these transfer caps based on the percentage of utility customers outside the city boundaries, as measured by total meters served. Under the bill, if more than:

- 15 percent of a municipal utility's customers are located outside of municipal boundaries, then the transfer rate applied to utility revenues will be reduced by 150 basis points.[17]
- 30 percent of a municipal utility's customers are located outside of municipal boundaries, then the transfer rate applied to utility revenues will be reduced by 300 basis points.
- 45 percent of a municipal utility's customers are located outside of municipal boundaries, then the transfer rate applied to utility revenues will be reduced by 450 basis points.

However, if a municipal utility is governed by a utility authority board that, through the election of voting members from outside the municipal boundaries, provides for representation of retail customers located outside the municipal boundaries approximately proportionate to the percentage of such customers, as measured by total meters served, then transfers of revenue are not subject to the above reductions.

The bill removes the provision allowing water or sewer utilities to add, for consumers outside of its boundaries, a surcharge of up to 25 percent of the rates, fees, and charges imposed on consumers within its boundaries. Furthermore, the bill changes the limit on the rates, fees, and charges such utility can impose on customers outside of municipal boundaries to no more than 25 percent above the total amount the municipal water or sewer utility charges customers within the municipal boundaries, provided rates for outside customers are set in a public hearing using the same methods as rates for other customers.

The bill limits the rates, fees, and charges that a municipal water or sewer utility that provides service to consumers within the boundaries of a separate municipality, using a water treatment plant or sewer treatment plant located within the boundaries of that separate municipality, by requiring that such charges are no more that the rates, fees, and charges imposed on consumers inside its own municipal boundaries.

The bill provides an effective date of July 1, 2024.

B. SECTION DIRECTORY:

**Section 1:** Amends s. 166.201, F.S., relating to taxes and charges.

**Section 2:** Amends s. 180.191, F.S., relating to limitation on rates charged consumer outside city limits.

[16] Section 367.081, F.S., permits the PSC to establish a leverage formula that reasonably reflect the range of returns on common equity for an average water or wastewater utility and which must be used to calculate the last authorized rate of return on equity for any utility which otherwise would have no established rate of return on equity.

[17] Basis points are commonly used to measure interest rates and percentages in finance, showing the change in the value or rate of a financial instrument, such as 1% change equals a change of 100 basis points and 0.01% change equals one basis point. Jason Fernando, *Basis Point (BPS) Explained for Interest Rates and Investments* (Jul. 5, 2022), Investopedia, https://www.investopedia.com/terms/b/basispoint.asp (last visited Mar. 20, 2023).

**Section 3:** Provides an effective date of July 1, 2024.

## II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

   None.

2. Expenditures:

   None.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

   The bill will likely have a negative fiscal impact on local governments which own and operate water or wastewater utilities, as it reduces the maximum amount that municipal water and sewer utilities can charge customers outside the municipal boundaries.

2. Expenditures:

   None.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

None.

D. FISCAL COMMENTS:

None.

## III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

   The county/municipality mandates provision of Art. VII, section 18(b), of the Florida Constitution may apply because this bill reduces the maximum amount that municipal water and sewer utilities can charge customers outside the municipal boundaries. If the bill does qualify as a mandate, final passage must be approved by two-thirds of the membership of each house of the Legislature.

2. Other:

   None.

B. RULE-MAKING AUTHORITY:

None.

C. DRAFTING ISSUES OR OTHER COMMENTS:

None.

## IV. AMENDMENTS/COMMITTEE SUBSTITUTE CHANGES

A bill to be entitled

An act relating to municipal utilities; amending s. 166.201, F.S.; authorizing a municipality to fund or finance general government functions with a portion of revenues from utility operations; establishing limits on utility revenue transfers for municipal utilities that serve customers located outside the municipal boundaries; amending s. 180.1291, F.S.; modifying provisions relating to permissible rates, fees, and charges imposed by municipal water and sewer utilities on customers located outside the municipal boundaries; providing an effective date.

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

Section 1. Section 166.201, Florida Statutes, is amended to read:

166.201 Taxes and charges.—

(1) A municipality may raise, by taxation and licenses authorized by the constitution or general law, or by user charges or fees authorized by ordinance, amounts of money which are necessary for the conduct of municipal government and may enforce their receipt and collection in the manner prescribed by ordinance not inconsistent with law.

(2)(a) A municipality that owns and operates an electric,



CODING: Words stricken are deletions; words underlined are additions.

natural gas, water, or wastewater utility may fund or finance general government functions using a portion of the revenues generated from rates, fees, and charges for the provision of such utility service. The portion of utility revenues that may be used during a fiscal year to fund or finance general government functions, after payment of all utility expenses, may not exceed:

1. For revenues generated from electric utility operations, a transfer rate equal to the amount derived by applying the average of the midpoints of the rates of return on equity approved by the Public Service Commission for each investor-owned electric utility in the state to the municipal electric utility's revenues.

2. For revenues generated from natural gas utility operations, a transfer rate equal to the amount derived by applying the average of the midpoints of the rates of return on equity approved by the Public Service Commission for each investor-owned natural gas utility in the state to the municipal natural gas utility's revenues.

3. For revenues generated from water or wastewater operations, a transfer rate equal to the amount derived by applying the rate of return on equity established by the Public Service Commission under s. 367.081(4)(f) to the municipal water or wastewater utility's revenues.

(b) Except as provided in paragraph (c), the transfer rate



CODING: Words stricken are deletions; words underlined are additions.

applied to municipal utility revenues under subparagraphs (a)1.-3. shall be reduced as follows:

1. If more than 15 percent of a municipal utility's retail customers, as measured by total meters served, are located outside the municipal boundaries, the transfer rate applied to utility revenues shall be reduced by 150 basis points.

2. If more than 30 percent of a municipal utility's retail customers, as measured by total meters served, are located outside the municipal boundaries, the transfer rate applied to utility revenues shall be reduced by 300 basis points.

3. If more than 45 percent of a municipal utility's retail customers, as measured by total meters served, are located outside the municipal boundaries, the transfer rate applied to utility revenues shall be reduced by 450 basis points.

(c) The reductions specified in paragraph (b) shall not apply to a municipal utility service if the utility service is governed by a utility authority board that, through the election of voting members from outside the municipal boundaries, provides for representation of retail customers located outside the municipal boundaries approximately proportionate to the percentage of such customers, as measured by total meters served, that receive service from the utility.

Section 2. Subsection (1) of section 180.191, Florida Statutes, is amended to read:

180.191 Limitation on rates charged consumer outside city



CODING: Words stricken are deletions; words underlined are additions.

limits.—

(1) Any municipality within the state operating a water or sewer utility outside of the boundaries of such municipality shall charge consumers outside the boundaries rates, fees, and charges determined in one of the following manners:

(a) It may charge the same rates, fees, and charges as consumers inside the municipal boundaries. ~~However, in addition thereto, the municipality may add a surcharge of not more than 25 percent of such rates, fees, and charges to consumers outside the boundaries.~~ Fixing of such rates, fees, and charges in this manner shall not require a public hearing except as may be provided for service to consumers inside the municipality.

(b)1. It may charge rates, fees, and charges that are just and equitable and which are based on the same factors used in fixing the rates, fees, and charges for consumers inside the municipal boundaries. ~~In addition thereto, the municipality may add a surcharge not to exceed 25 percent of such rates, fees, and charges for said services to consumers outside the boundaries. However, the total of all such~~ Such rates, fees, and charges for the services to consumers outside the boundaries shall not be more than 25 ~~50~~ percent greater than ~~in excess of~~ the total amount the municipality charges consumers served within the municipality for corresponding service. No such rates, fees, and charges shall be fixed until after a public hearing at which all of the users of the water or sewer systems;



CODING: Words ~~stricken~~ are deletions; words underlined are additions.

owners, tenants, or occupants of property served or to be served thereby; and all others interested shall have an opportunity to be heard concerning the proposed rates, fees, and charges. Any change or revision of such rates, fees, or charges may be made in the same manner as such rates, fees, or charges were originally established, but if such change or revision is to be made substantially pro rata as to all classes of service, both inside and outside the municipality, no hearing or notice shall be required.

(2) Any municipality within the state operating a water or sewer utility that provides service to consumers within the boundaries of a separate municipality through the use of a water treatment plant or sewer treatment plant located within the boundaries of that separate municipality may charge consumers in the separate municipality no more than the rates, fees, and charges imposed on consumers inside its own municipal boundaries.

Section 3. This act shall take effect July 1, 2024.



CODING: Words stricken are deletions; words underlined are additions.