HOUSE OF REPRESENTATIVES STAFF FINAL BILL ANALYSIS

BILL #: CS/HB 1639 Pub. Rec./Network Schematics, Hardware and Software Configurations, or Encryption/Supervisors of Elections
SPONSOR(S): Government Operations Subcommittee; Grant
TIED BILLS: **IDEN./SIM. BILLS:** CS/SB 1704

FINAL HOUSE FLOOR ACTION: 117 **Y's** 0 **N's** **GOVERNOR'S ACTION:** Approved

SUMMARY ANALYSIS

CS/HB 1639 passed the House on April 21, 2021, and subsequently passed the Senate on April 22, 2021.

Supervisors of elections (supervisors) are elected constitutional officers and serve a four-year term. Each county has a supervisor who conducts elections within his or her county. Accordingly, various duties relating to elections and voter registration are assigned to the supervisor.

The Information Technology (IT) Security Act requires the Department of Management Services and the heads of state agencies to meet certain requirements to enhance the IT security of state agencies. Under the Act, portions of records held by a state agency relating to IT security are confidential and exempt from public record requirements. However, this public record exemption does not apply to records of the supervisor.

The bill creates a public record exemption for portions of records held by a supervisor that contain network schematics, hardware and software configurations, or encryption, or which identify detection, investigation, or response practices for suspected or confirmed IT security incidents. The bill provides that the confidential and exempt records must be made available to the Auditor General and may be made available to another governmental entity for IT security purposes or in the furtherance of the entity's official duties.

The bill provides for retroactive application of the public record exemption. It also provides that the exemption is subject to the Open Government Sunset Review Act and will repeal on October 2, 2026, unless reviewed and saved from repeal by the Legislature.

The bill may have a minimal fiscal impact on supervisors responsible for complying with public record requests and redacting confidential and exempt information prior to releasing a record.

The bill was approved by the Governor on June 4, 2021, ch. 2021-73, L.O.F., and became effective on that date.

I. SUBSTANTIVE INFORMATION

A. EFFECT OF CHANGES:

Public Records

Article I, s. 24(a) of the Florida Constitution sets forth the state's public policy regarding access to government records. This section guarantees every person a right to inspect or copy any public record of the legislative, executive, and judicial branches of government; counties, municipalities, and districts; and each constitutional officer, board, and commission, or entity created pursuant to law or the Florida Constitution. The Legislature, however, may provide by general law for the exemption of records from the requirements of art. I, s. 24(a) of the Florida Constitution.[1] The general law must state with specificity the public necessity justifying the exemption[2] and must be no broader than necessary to accomplish its purpose.[3]

Public policy regarding access to government records is addressed further in s. 119.07(1)(a), F.S., which guarantees every person a right to inspect and copy any state, county, or municipal record, unless the record is exempt. Furthermore, the Open Government Sunset Review Act[4] provides that a public record or public meeting exemption may be created 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.[5]

The Open Government Sunset Review Act requires the automatic repeal of a newly created public record exemption on October 2nd of the fifth year after creation or substantial amendment, unless the Legislature reenacts the exemption.[6]

Information Technology Security Act

The Information Technology (IT) Security Act[7] requires the Department of Management Services (DMS) and the heads of state agencies[8] to meet certain requirements to enhance the IT security of state agencies. Specifically, the IT Security Act provides that DMS is responsible for establishing standards and processes consistent with generally accepted best practices for IT security,[9] including cybersecurity, and adopting rules that safeguard an agency's data, information, and IT resources to ensure availability, confidentiality, and integrity and to mitigate risks.[10]

---

[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] Section 119.15, F.S.
[5] Section 119.15(6)(b), F.S.
[6] Section 119.15(3), F.S.
[7] Section 282.318, F.S.
[8] 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. Section 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. Section 282.318(2), F.S.
[9] 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. Section 282.0041(22), F.S.
[10] Section 292.318(3), F.S.

The IT Security Act provides a public record exemption for portions of records held by a state agency that contain network schematics, hardware and software configurations, or encryption, or which identify detection, investigation, or response practices for suspected or confirmed information technology security incidents, including suspected or confirmed breaches, if the disclosure of such records would facilitate unauthorized access to or the unauthorized modification, disclosure, or destruction of:

- Data or information, whether physical or virtual; or
- IT resources, which includes:
    - Information relating to the security of the agency's technologies, processes, and practices designed to protect networks, computers, data processing software, and data from attack, damage, or unauthorized access; or
    - Security information, whether physical or virtual, which relates to the agency's existing or proposed IT systems.[11]

Supervisors of Elections

Supervisors of elections (supervisors) are elected constitutional officers and serve a four-year term.[12] Each county has a supervisor who conducts elections within his or her county. Accordingly, various duties relating to elections and voter registration are assigned to the supervisor, including:

- Updating voter registration information.
- Acting as the official custodian of documents related to the registration of electors and changes in voter registration status of electors.
- Maintaining an office that must be open during certain hours.
- Ensuring all voter registration procedures and systems comply with applicable requirements.
- Providing training to certain officials relating to elections.
- Appointing an election board.[13]

Supervisors do not have a public record exemption for certain IT security records.

Effect of the Bill

The bill creates a public record exemption for certain IT security records held by a supervisor that is similar to the public record exemption currently provided to state agencies. Specifically, the bill provides that portions of records held by a supervisor that contain network schematics, hardware and software configurations, or encryptions, or which identify detection, investigation, or response practices for suspected or confirmed IT security incidents, including suspected or confirmed breaches are confidential and exempt[14] from public record requirements if the disclosure of such records would facilitate unauthorized access to or the unauthorized modification, disclosure, or destruction of:

- Data or information, whether physical or virtual; or
- IT resources,[15] which includes:
    - Information relating to the security of a supervisor's technology, processes, and practices designed to protect networks, computers, data processing software, and data from attack, damage, or unauthorized access; or

[11] Section 282.318(5), F.S.
[12] Article VIII, s. 1(d), FLA. CONST.
[13] *See* chs. 98 and 102, F.S.
[14] 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).
[15] The term "information technology resources" means data processing hardware and software and services, communications, supplies, personnel, facility resources, maintenance, and training. Section 119.011(9), F.S.

- Security information, whether physical or virtual, which relates to a supervisor's existing or proposed IT systems.

The bill provides that the confidential and exempt records must be available to the Auditor General and may be made available to another governmental entity for IT security purposes or in the furtherance of the entity's official duties.

The bill provides a public necessity statement as required by art. I, s. 24(c) of the Florida Constitution. The public necessity statement states that if the above protected information was released, it could be used as a tool to influence elections, frustrate the voting process, manipulate election results, or otherwise interfere with the administration of elections, and result in increased security breaches and fraud impacting the election process.

The bill provides for retroactive application of the public record exemption. It also provides that the exemption is subject to the Open Government Sunset Review Act and will repeal on October 2, 2026, unless reviewed and saved from repeal by the Legislature.

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.

2. Expenditures:

   The bill may have a minimal fiscal impact on supervisors responsible for complying with public record requests and redacting confidential and exempt information prior to releasing a record. Such costs, however, would be absorbed as part of the day-to-day responsibilities of these officers.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

None.

D. FISCAL COMMENTS:

None.