FLORIDA HOUSE OF REPRESENTATIVES
FINAL BILL ANALYSIS

This bill analysis was prepared by nonpartisan committee staff and does not constitute an official statement of legislative intent.

BILL #: HB 7023 PCB GOS 26-09	**COMPANION BILL:** SB 7024
TITLE: OGSR/Cybersecurity	**LINKED BILLS:** None
SPONSOR(S): Government Operations Subcommittee, Conerly	**RELATED BILLS:** None

FINAL HOUSE FLOOR ACTION: 107 **Y's** 0 **N's** **GOVERNOR'S ACTION:** Pending

SUMMARY

Effect of the Bill:
The bill expands the current cybersecurity public record and public meeting exemption applicable to all agencies—state and local—by incorporating the following cybersecurity-related exemptions that currently apply to specific agencies:

- Information relating to processes or practices designed to protect data, information, or existing or proposed information technology or operational technology.
- Portions of risk assessments, evaluations, audits, and other reports of an agency's cybersecurity program.
- Login credentials.
- Internet protocol addresses, geolocation data, and other information describing how and when users access public-facing portals.

The bill provides for repeal of the exemption on October 2, 2031, unless reviewed and reenacted by the Legislature.

Fiscal or Economic Impact:
The bill may have an insignificant, negative fiscal impact on the state and local governments.

JUMP TO SUMMARY ANALYSIS RELEVANT INFORMATION

ANALYSIS

EFFECT OF THE BILL:

HB 7023 passed as SB 7024.

The bill expands the current cybersecurity public record and public meeting exemption applicable to all state and local governmental agencies to incorporate cybersecurity-related exemptions that currently apply to specific agencies. The existing general cybersecurity public record and public meeting exemption was reviewed pursuant to the Open Government Sunset Review Act (OGSR Act) and the exemptions will repeal on October 2, 2026, if this bill does not become a law. (Section 1)

The bill revises the existing general cybersecurity[1] public record and public meeting exemption to include the following categories of information:

- Network schematics, hardware and software configurations, encryption information, or information identifying detection, investigation, or response practices related to cybersecurity incidents,[2] including breaches,[3] if disclosure could facilitate unauthorized access to or unauthorized modification, disclosure, or

[1] The bill defines "cybersecurity" to mean the protection afforded to information technology or operational technology in order to attain the applicable objectives of preserving the confidentiality, integrity, and availability of those technologies, data, and information.
[2] The bill defines "incident" to mean a violation or imminent threat of violation, whether such violation is accidental or deliberate, of an agency's cybersecurity, information technology, or operational technology.
[3] The bill defines "breach" to mean unauthorized access of data or information. Good faith access of data or information by an employee or agent of an agency does not constitute a breach, provided that the data or information is not used for a purpose unrelated to the business or subject to further unauthorized use.

destruction of data, information, or existing or proposed information technology (IT) or operational technology (OT).
- Information relating to processes or practices designed to protect data, information, or existing or proposed IT or OT if disclosure could facilitate unauthorized access to or unauthorized modification, disclosure, or destruction of such data, information, or technology.
- Portions of risk assessments, evaluations, audits, and other reports of an agency's cybersecurity program if disclosure could facilitate unauthorized access to or unauthorized modification, disclosure, or destruction of data, information, or existing or proposed IT or OT.
- Login credentials.[4]
- Internet protocol addresses, geolocation data, and other information that describes the location, computer, computer system, or computer network from which a user accesses a public-facing portal,[5] and the dates and times that a user accesses a public-facing portal.
- Sensitive agency-produced data processing software.
- Insurance and self-insurance coverage limits and deductibles, and other risk mitigation coverages, acquired for the protection of IT, OT, or data of an agency. (Section 1)

The bill maintains the existing exemptions for information relating to critical infrastructure and for cybersecurity incident information reported pursuant to law. (Section 1)

Any portion of a public meeting that would reveal the confidential and exempt cybersecurity information is exempt from public meeting requirements and any portion of an exempt meeting must be recorded and transcribed. The recording and transcript of the exempt portion of the meeting are confidential and exempt from public record requirements. (Section 1)

With one exception, the bill maintains existing requirements and permissions governing disclosure of the confidential and exempt information. The bill revises the provision authorizing disclosure to another agency or governmental entity to allow disclosure in the furtherance of that agency's or governmental entity's *official* duties and responsibilities, rather than its *statutory* duties and responsibilities. (Section 1)

The bill provides that the exemptions apply to information held by an agency before, on, or after the effective date of the act. Pursuant to the OGSR Act, these exemptions will automatically repeal on October 2, 2031, unless reviewed and saved from repeal by the Legislature. (Section 1)

The bill includes the constitutionally required public necessity statement, which finds that disclosure of the sensitive cybersecurity information protected by the bill could place an agency at greater risk of breaches, cybersecurity incidents, and ransomware attacks and could significantly impair the administration of vital governmental programs. (Section 14)

The bill deletes agency-specific public record and public meeting exemptions that are incorporated into the general cybersecurity exemption and makes other conforming changes. If the bill does not become law, the general cybersecurity exemption and two agency-specific exemptions—one regarding certain IT information held by the Department of Highway Safety and Motor Vehicles and one regarding agency cybersecurity risk assessments and audits—will repeal on October 2, 2026. (Multiple Sections)

Subject to the Governor's veto powers, the effective date of this bill is upon becoming a law. (Section 16)

[4] The bill defines "login credentials" to mean information used to authenticate a user's identity or otherwise authorize access when logging into a computer, computer system, computer network, electronic device, or an online user account accessible over the Internet through a mobile device, a website, or any other electronic means, or for authentication or password or account recovery.
[5] The bill defines "public-facing portal" to mean a web portal or computer application accessible by the public over the Internet, whether through a mobile device, website, or other electronic means.

FISCAL OR ECONOMIC IMPACT:

STATE GOVERNMENT:

The bill will likely have an insignificant, negative fiscal impact on the state. Agencies may incur minor costs associated with training staff to implement the expanded public record exemption as well as with redacting confidential and exempt information before the release of records. These costs are expected to be absorbed within existing resources.

LOCAL GOVERNMENT:

The bill will likely have an insignificant, negative fiscal impact on local governments. Local governments may incur minor costs associated with training staff to implement the expanded public record exemption as well as with redacting confidential and exempt information before the release of records. These costs are expected to be absorbed within existing resources.

RELEVANT INFORMATION

SUBJECT OVERVIEW:

Open Government Sunset Review Act

The Open Government Sunset Review Act (OGSR Act)[6] sets forth a legislative review process for newly created or substantially amended public record or public meeting exemptions. It requires an automatic repeal of the exemption on October 2nd of the fifth year after creation or substantial amendment, unless the Legislature reenacts the exemption.[7]

The OGSR Act 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 is 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; or
- Protect trade or business secrets.[8]

If in reenacting an exemption that will repeal, the exemption is expanded, then a public necessity statement and a two-thirds vote for passage are required. If the exemption is reenacted with grammatical or stylistic changes that do not expand the exemption, if the exemption is narrowed, or if an exception to the exemption is created, then a public necessity statement and a two-thirds vote are not required.[9]

Cybersecurity-related Exemptions

The Legislature has enacted multiple agency-specific[10] public record and public meeting exemptions to protect cybersecurity-related information from disclosure. The purpose of these exemptions is to prevent the release of information that could compromise government information technology (IT),[11] operational technology (OT),[12] and

[6] S. 119.15, F.S.
[7] S. 119.15(3), F.S.
[8] S. 119.15(6)(b), F.S.
[9] *See* Art. I, s. 24(c), FLA. CONST.
[10] "Agency" means any state, county, district, authority, or municipal officer, department, division, board, bureau, commission, or other separate unit of government created or established by law including, the Commission on Ethics, the Public Service Commission, and the Office of Public Counsel, and any other public or private agency, person, partnership, corporation, or business entity acting on behalf of any public agency. S. 119.011(2), F.S.
[11] "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,

related systems and data. While these agency-specific exemptions address a similar public purpose, they are dispersed across multiple chapters of law and vary in scope and terminology. These exemptions currently protect the following information:

- Secure login credentials held by the Department of State (DOS) relating to certain password-protected systems.[13]
- User identifications and passwords held by DOS relating to the electronic filing system for campaign finance reports.[14]
- Information relating to the Department of the Lottery's cybersecurity technologies, processes, and practices designed to protect its IT systems and data.[15]
- Secure login credentials held by the Commission on Ethics relating to the electronic filing system for financial interest disclosures.[16]
- Sensitive agency-produced data processing software.[17]
- Secure login credentials, Internet protocol addresses, geolocation data, and other information that describes the location, computer, computer system, or computer network from which a user accesses a public-facing portal, and the dates and times that a user accesses a public-facing portal, held by the Department of Highway Safety and Motor Vehicles.[18]
- Information relating to a local government owned or operated utility's security processes and practices designed to protect its IT or industrial control technology systems.[19]
- Cybersecurity policies and procedures, audits, risk assessments, evaluations, and other reports of a state agency's cybersecurity program.[20]
- Risk assessments, evaluations, audits, and other reports of Citizens Property Insurance Corporation's cybersecurity program.[21]
- Information identifying detection, investigation, or response practices, and risk assessments, evaluations, audits, and other reports, relating to the cybersecurity program of a state university or Florida College System Institution.[22]

---

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(20), F.S.

[12] "Operational technology" means the hardware and software that cause or detect a change through the direct monitoring or control of physical devices, systems, processes, or events. S. 119.0725(1)(g), F.S.

[13] S. 15.16(3)(c)2., F.S.

[14] S. 106.0706(1), F.S.

[15] *See* s. 24.1051(1)(a)1.a., F.S.

[16] S. 112.31446(6)(a), F.S.

[17] S. 119.071(1)(f), F.S. This exemption currently applies to all agencies.

[18] S. 119.0712(2)(f), F.S.

[19] *See* s. 119.0713(5)(a)1.-2., F.S.

[20] *See* s. 282.318(4)-(9), F.S.

[21] S. 627.352, F.S.

[22] *See* s. 1004.055, F.S.

Public Record and Public Meeting Exemption under Review

In 2022, the Legislature created a public record exemption applicable to all agencies—state and local—for certain cybersecurity-related information.[23] Specifically, it provides that the following information is confidential and exempt[24] from public record requirements:

- Coverage limits, deductible, or self-insurance amounts for cybersecurity insurance or other risk mitigation coverages protecting an agency's IT systems, OT systems, or data.
- Information relating to critical infrastructure.[25]
- Network schematics, hardware and software configurations, encryption information, or information identifying detection, investigation, or response practices for suspected or confirmed cybersecurity incidents, including suspected or confirmed breaches, if disclosure would enable unauthorized access, modification, disclosure, or destruction of:
  - Data or information, whether physical or virtual; or
  - IT resources, including existing or proposed agency IT systems.
- Cybersecurity incident information reported pursuant to law.[26]

The Legislature also created a public meeting exemption for any portion of a meeting that would reveal the confidential and exempt information, and required any portion of an exempt meeting to be recorded and transcribed. The recording and transcript are confidential and exempt from public record requirements.[27]

The confidential and exempt information must be made available to law enforcement agencies, the Auditor General, the Cybercrime Office, the Florida Digital Service, and, for agencies under the jurisdiction of the Governor, the Chief Inspector General, and may be made available by an agency in the furtherance of its official duties and responsibilities or to another governmental entity in the furtherance of its statutory duties and responsibilities. In addition, information about cybersecurity incidents may be reported in the aggregate.[28]

The 2022 public necessity statement[29] provided that:

> Release of such information could place an agency at greater risk of breaches, cybersecurity incidents, and ransomware attacks. . . Therefore, this information should be made confidential and exempt in order to protect the agency's data, information, and information technology resources. [Furthermore,] failure to close that portion of a meeting at which confidential and exempt information would be revealed, and prevent the disclosure of the recordings and transcripts of those portions of a meeting, would defeat the purpose of the underlying public records exemption and could result in the release of highly sensitive information related to the cybersecurity of an agency system.

---

[23] *See* s. 119.0725, F.S.

[24] There is a difference between records the Legislature designates *exempt* from public record requirements and those the Legislature designates *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); *State v. Wooten*, 260 So. 3d 1060, 1070 (Fla. 4th DCA 2018); *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. 04-09 (2004).

[25] "Critical infrastructure" means existing and proposed IT and OT systems and assets, whether physical or virtual, the incapacity or destruction of which would negatively affect security, economic security, public health, or public safety. S. 119.0725(1)(b), F.S.

[26] S. 119.0725(2), F.S. The exemption applies to information held by an agency before, on, or after July 1, 2022, which was the effective date of the exemption's initial codification in law. *See* s. 119.0724(4), F.S.

[27] S. 119.0725(3), F.S.

[28] S. 119.0725(5) and (6), F.S.

[29] Article I, s. 24(c), FLA CONST., requires each public record and public meeting exemption to "state with specificity the public necessity justifying the exemption."

Pursuant to the OGSR Act, the public record and public meeting exemption will repeal on October 2, 2026,[30] unless reenacted by the Legislature.[31]

During the 2026 interim, House and Senate committee staff surveyed state agencies, universities, counties, and municipalities regarding the public record and public meeting exemption under review. In total, staff received 172 responses.[32] Respondents indicated they were unaware of any litigation concerning the exemption, and the vast majority of respondents recommended the exemption be reenacted as is. As part of the questionnaire, respondents were asked whether any agency-specific cybersecurity-related exemptions should be incorporated into the general cybersecurity exemption. Some respondents suggested merging agency-specific exemptions into the general exemption, while others suggested maintaining the status quo.

[30] In 2025, the Legislature revised the OGSR review date from October 2, 2027, to October 2, 2026, to align the review of the general cybersecurity exemption with the review of other cybersecurity-related exemptions. *See* ch. 2025-27, L.O.F.
[31] S. 119.0725(7), F.S.
[32] Open Government Sunset Review Questionnaire, *Agency Cybersecurity Information*, responses on file with the Government Operations Subcommittee.