

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 #: [CS/HB 7013](#) [PCB GOS 25-05](#)

TITLE: OGSR/Cybersecurity

SPONSOR(S): Government Operations Subcommittee;
Greco

COMPANION BILL: [SB 7020](#) (Fine)

LINKED BILLS: None

RELATED BILLS: None

FINAL HOUSE FLOOR ACTION: 116 Y's

0 N's

GOVERNOR'S ACTION: Approved

SUMMARY

Effect of the Bill:

The bill aligns the repeal dates required under the Open Government Sunset Review Act for certain cybersecurity-related public record and public meeting exemptions, and provides that the exemptions will repeal on October 2, 2027.

Fiscal or Economic Impact:

None.

[JUMP TO](#)

[SUMMARY](#)

[ANALYSIS](#)

[RELEVANT INFORMATION](#)

ANALYSIS

EFFECT OF THE BILL:

CS/HB 7013 passed as [SB 7020](#). (Please note that bill section parentheticals do not contain hyperlinks to bill sections for Senate bills.)

The bill adjusts the scheduled repeal dates, created pursuant to the [Open Government Sunset Review Act](#), for certain cybersecurity-related public record and public meeting exemptions. Specifically, the bill moves the repeal date of the [general cybersecurity public record and public meeting exemption](#) from October 2, 2027, to October 2, 2026, and extends the public record and public meeting exemption for [risk assessments, evaluations, external audits, and other reports](#) of a state agency's cybersecurity program from October 2, 2025, to October 2, 2026. These changes align the repeal dates for both exemptions to provide for simultaneous review next year. (Sections 1 and 2)

The bill was approved by the Governor on May 16, 2025, ch. 2025-27, L.O.F., and will become effective on July 1, 2025. (Section 3)

RELEVANT INFORMATION

SUBJECT OVERVIEW:

[Open Government Sunset Review \(OGSR\) Act](#)

The OGSR Act¹ 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.²

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.

¹ S. [119.15, F.S.](#)

² S. [119.15\(3\), F.S.](#)

STORAGE NAME: h7013z1.GOS

DATE: 5/20/2025

- 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.³

If, and only 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.⁴ 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 for passage are not required.

General Cybersecurity Public Record and Public Meeting Exemption

In 2022, the Legislature created a public record exemption applicable to all agencies⁵—state and local—for certain cybersecurity-related information.⁶ Specifically, it provides that the following information is confidential and exempt⁷ from public record requirements:

- Coverage limits, deductible, or self-insurance amounts for cybersecurity insurance or other risk mitigation coverages protecting an agency's information technology (IT) systems, operational technology (OT)⁸ systems, or data.
- Information relating to critical infrastructure.⁹
- Network schematics, hardware and software configurations, encryption information, and cybersecurity practices for detecting, investigating, or responding to incidents, including suspected or confirmed breaches, if disclosure could 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.¹⁰

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.¹¹

The foregoing confidential and exempt information must be made available to law enforcement agencies, the Auditor General, the Cybercrime Office, the Florida Digital Service (FLDS), 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 duties and responsibilities or to another governmental entity in the furtherance of its duties and responsibilities. In addition, information about cybersecurity incidents may be reported in the aggregate.¹²

³ S. [119.15\(6\)\(b\), F.S.](#)

⁴ [Art. I, s. 24\(c\), FLA. CONST.](#)

⁵ "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.](#)

⁶ S. [119.0725, F.S.](#)

⁷ 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).

⁸ "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.](#)

⁹ "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.](#)

¹⁰ S. [119.0725\(2\), F.S.](#)

¹¹ S. [119.0725\(3\), F.S.](#)

¹² S. [119.0725\(5\) and \(6\), F.S.](#)

Pursuant to the OGSR Act, the general public record and public meeting exemption for cybersecurity-related information will repeal on October 2, 2027, unless reviewed and saved from repeal by the Legislature.¹³

Public Record and Public Meeting Exemptions under Review

In 2016, the Legislature created a public record exemption for certain portions of [risk assessments, evaluations, external audits,](#)¹⁴ [and other reports](#) of a state agency's cybersecurity program. Such records are confidential and exempt from public record requirements, but only to the extent that disclosure would facilitate unauthorized access, modification, disclosure, or destruction of:

- Data or information, whether physical or virtual; or
- IT resources, including existing or proposed IT systems.¹⁵

The 2016 public necessity statement¹⁶ for the public record exemption provided that:

Such documents would likely include an analysis of the state agency's current information technology program or systems which could clearly identify vulnerabilities or gaps in current systems or processes and propose recommendations to remedy identified vulnerabilities. The disclosure of such portions of records would jeopardize the information technology security of the state agency, and compromise the integrity and availability of agency data and information technology resources, which would significantly impair the administration of governmental programs.

In 2020, the Legislature created a complementary public meeting exemption for those portions of a public meeting that would reveal the confidential and exempt information protected by the public record exemption.¹⁷ The public meeting exemption requires the exempt portions of such meetings be recorded and transcribed. The recording and transcript are confidential and exempt from public record requirements unless a court of competent jurisdiction determines that the meeting was not restricted to the discussion of confidential and exempt information.

The 2020 public necessity statement for the public meeting exemption provided that:

Such meetings must be made exempt from open meetings requirements in order to protect agency information technology systems, resources, and data. This information would clearly identify a state agency's information technology systems and its vulnerabilities and disclosure of such information would jeopardize the information technology security of the state agency and compromise the integrity and availability of state agency data and information technology resources. Such disclosure would significantly impair the administration of state programs.

The confidential and exempt information must be made available to the Auditor General, the Cybercrime Office, FLDS, and, for agencies under the jurisdiction of the Governor, the Chief Inspector General. Such information 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.¹⁸

Pursuant to the OGSR Act, the public record and public meeting exemption will repeal on October 2, 2025, unless saved from repeal by the Legislature.

¹³ S. [119.0725\(7\), F.S.](#)

¹⁴ "External audit" means an audit that is conducted by an entity other than the state agency that is the subject of the audit. [S. 282.318\(5\), F.S.](#)

¹⁵ Ch. [2016-114, L.O.F.](#), codified as [s. 282.318\(5\), F.S.](#)

¹⁶ [Art. I, s. 24\(c\), FLA CONST.](#), requires each public record exemption to "state with specificity the public necessity justifying the exemption."

¹⁷ Ch. [2020-25, L.O.F.](#), codified as s. [282.318\(6\), F.S.](#)

¹⁸ S. [282.318\(7\), F.S.](#)

During the 2024 interim, House and Senate committee staff jointly sent questionnaires to state agencies regarding the exemptions. In total, staff received 27 responses from those entities.¹⁹ The respondents indicated they were unaware of any litigation concerning the exemptions under review and the vast majority recommended that the exemptions be reenacted as is. As a part of the questionnaire, respondents were asked whether the exemptions were duplicative of the general cybersecurity public record and public meeting exemption. Some respondents noted there may be overlap between the exemptions.

RECENT LEGISLATION:

YEAR	BILL #	HOUSE SPONSOR(S)	SENATE SPONSOR	OTHER INFORMATION
2022	CS/HB 7057	Giallombardo	Hutson	Passed and became law.

¹⁹ Open Government Sunset Review Questionnaire, Public Records and Public Meetings Related to Cybersecurity Risk Assessments and Audits, responses on file with the Government Operations Subcommittee.