A bill to be entitled

An act relating to a review under the Open Government Sunset Review Act; amending s. 119.0725, F.S.; providing and revising definitions; providing an exemption from public records requirements for certain cybersecurity processes or practices, certain cybersecurity program reports, login credentials, and certain information associated with access to a public-facing portal held by an agency; revising an exemption from public records requirements for certain cybersecurity insurance information and certain cybersecurity-related information held by an agency; consolidating a public record exemption for certain agency-produced data processing software held by an agency; expanding an exemption from public meetings requirements for portions of a meeting that would reveal certain cybersecurity-related information held by an agency; providing for future legislative review and repeal of the exemptions; amending s. 15.16, F.S.; removing an exemption from public records requirements for certain secure login credentials held by the Department of State; amending s. 24.1051, F.S.; removing an exemption from public records requirements for certain cybersecurity-related information held by the Department of the Lottery; amending s. 101.5607,

F.S.; conforming a provision to changes made by the act; amending s. 106.0706, F.S.; removing an exemption from public records requirements for certain user identifications and passwords held by the Department of State; amending s. 112.31446, F.S.; removing an exemption from public records requirements for certain secure login credentials held by the Commission on Ethics; amending s. 119.07, F.S.; conforming a provision to changes made by the act; amending s. 119.071, F.S.; removing an exemption from public records requirements for certain agency-produced data processing software; amending s. 119.0712, F.S.; removing an exemption from public records requirements for certain secure login credentials and certain information associated with access to a public-facing portal held by the Department of Highway Safety and Motor Vehicles; amending s. 119.0713, F.S.; removing an exemption from public records requirements for certain cybersecurity-related information held by a utility owned or operated by a unit of local government; amending s. 119.0714, F.S.; conforming a provision to changes made by the act; amending s. 282.318, F.S.; removing an exemption from public records requirements for a comprehensive risk assessment held by an agency; removing exemptions from

public records requirements for certain cybersecurity-related internal policies and procedures, certain cybersecurity-related internal audits and evaluations held by an agency, and certain cybersecurity-related reports held by an agency; repealing s. 627.352, F.S., relating to security of data and information technology in Citizens Property Insurance Corporation; repealing s. 1004.055, F.S., relating to security of data and information technology in state postsecondary education institutions; providing a statement of public necessity; providing an effective date.

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

Section 1. Paragraphs (a), (c), (e), and (g) of subsection (1), subsections (2) and (4), paragraph (b) of subsection (5), and subsection (7) of section 119.0725, Florida Statutes, are amended, and new paragraphs (g) and (i) are added to subsection (1) of that section, to read:

119.0725 Agency cybersecurity information; public records exemption; public meetings exemption.—

(1) As used in this section, the term:

(a) "Breach" means unauthorized access of data or information ~~in electronic form containing personal information~~. Good faith access of data or information ~~personal 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.

(c) "Cybersecurity" means 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 ~~has the same meaning as in s. 282.0041~~.

(e) "Incident" means a violation or imminent threat of violation, whether such violation is accidental or deliberate, of an agency's cybersecurity, information technology ~~resources~~, or operational technology ~~security, policies, or practices~~. As used in this paragraph, the term "imminent threat of violation" means a situation in which the agency has a factual basis for believing that a specific incident is about to occur.

(g) "Login credentials" means 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.

(h) ~~(g)~~ "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.

(i) "Public-facing portal" means a web portal or computer application accessible by the public over the Internet, whether through a mobile device, website, or other electronic means.

(2) The following information held by an agency is confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution:

~~(a) Coverage limits and deductible or self-insurance amounts of insurance or other risk mitigation coverages acquired for the protection of information technology systems, operational technology systems, or data of an agency.~~

(a) ~~(b)~~ Information relating to critical infrastructure.

(b) ~~(c)~~ Cybersecurity incident information reported pursuant to s. 282.318 or s. 282.3185.

(c) ~~(d)~~ Network schematics, hardware and software configurations, ~~or~~ encryption information, or any information that identifies detection, investigation, or response practices related to ~~for suspected or confirmed~~ cybersecurity incidents, including ~~suspected or confirmed~~ breaches, if the disclosure of such information could ~~would~~ facilitate unauthorized access to or unauthorized modification, disclosure, or destruction of data, information, or existing or proposed information technology or operational technology.

(d) Information relating to processes or practices designed to protect data, information, or existing or proposed information technology or operational technology if the disclosure of such information could facilitate unauthorized access to or unauthorized modification, disclosure, or destruction of such data, information, or technology.

(e) Portions of risk assessments, evaluations, audits, and other reports of an agency's cybersecurity program if the disclosure of such information could facilitate unauthorized access to or unauthorized modification, disclosure, or destruction of data, information, or existing or proposed information technology or operational technology.

(f) Login credentials.

(g) 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.

(h) Agency-produced data processing software that is sensitive.

(i) Insurance and self-insurance coverage limits and deductibles, as well as any other risk mitigation coverages, acquired for the protection of information technology, operational technology, or data of an agency.÷

~~1. Data or information, whether physical or virtual; or~~

~~2. Information technology resources, which include an agency's existing or proposed information technology systems.~~

(4) The public records exemptions contained in this section apply to information held by an agency before, on, or after the effective date of this act ~~July 1, 2022~~.

(5)

(b) Such confidential and exempt information may be disclosed by an agency in the furtherance of its official duties and responsibilities or to another agency or governmental entity in the furtherance of the agency's or governmental entity's official ~~its statutory~~ duties and responsibilities.

(7) This section is subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2031 ~~October 2, 2026~~, unless reviewed and saved from repeal through reenactment by the Legislature.

Section 2. Paragraph (c) of subsection (3) of section 15.16, Florida Statutes, is amended to read:

15.16 Reproduction of records; admissibility in evidence; electronic receipt and transmission of records; certification; acknowledgment.—

(3)

(c)1. E-mail addresses collected by the Department of State pursuant to this subsection are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution. This exemption applies to e-mail addresses held by the Department of State

before, on, or after the effective date of the exemption.

~~2. Secure login credentials held by the Department of State for the purpose of allowing a person to electronically file records under this subsection are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution. This exemption applies to secure login credentials held by the Department of State before, on, or after the effective date of the exemption. For purposes of this subparagraph, the term "secure login credentials" means information held by the department for purposes of authenticating a user logging into a user account on a computer, a computer system, a computer network, or an electronic device; an online user account accessible over the Internet, whether through a mobile device, a website, or any other electronic means; or information used for authentication or password recovery.~~

2.~~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 3. Paragraph (a) of subsection (1) of section 24.1051, Florida Statutes, is amended to read:

24.1051 Exemptions from inspection or copying of public records.—

(1)(a) The following information held by the department is confidential and exempt from s. 119.07(1) and s. 24(a), Art. I

of the State Constitution:

1. Information that, if released, could harm the security or integrity of the department, including:

~~a. Information relating to the security of the department's technologies, processes, and practices designed to protect networks, computers, data processing software, data, and data systems from attack, damage, or unauthorized access. This sub-subparagraph is subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2027, unless reviewed and saved from repeal through reenactment by the Legislature.~~

a.~~b.~~ Security information or information that would reveal security measures of the department, whether physical or virtual.

b.~~c.~~ Information about lottery games, promotions, tickets, and ticket stock, including information concerning the description, design, production, printing, packaging, shipping, delivery, storage, and validation of such games, promotions, tickets, and stock.

c.~~d.~~ Information concerning terminals, machines, and devices that issue tickets.

2. Information that must be maintained as confidential in order for the department to participate in a multistate lottery association or game.

3. Personal identifying information obtained by the

department when processing background investigations of current or potential retailers or vendors.

4. Financial information about an entity which is not publicly available and is provided to the department in connection with its review of the financial responsibility of the entity pursuant to s. 24.111 or s. 24.112, provided that the entity marks such information as confidential. However, financial information related to any contract or agreement, or an addendum thereto, with the department, including the amount of money paid, any payment structure or plan, expenditures, incentives, bonuses, fees, and penalties, shall be public record.

Section 4. Paragraph (d) of subsection (1) of section 101.5607, Florida Statutes, is amended to read:

101.5607 Department of State to maintain voting system information; prepare software.—

(1)

(d) Section 119.0725(2)(h) ~~Section 119.071(1)(f)~~ applies to all software on file with the Department of State.

Section 5. Section 106.0706, Florida Statutes, is amended to read:

106.0706 Electronic filing of campaign finance reports; public records exemption.—

~~(1) All user identifications and passwords held by the Department of State pursuant to s. 106.0705 are confidential and~~

~~exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution.~~

(1)~~(2)(a)~~ Information entered in the electronic filing system for purposes of generating a report pursuant to s. 106.0705 is exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution.

(2)~~(b)~~ Information entered in the electronic filing system is no longer exempt once the report is generated and filed with the Division of Elections.

Section 6. Subsection (6) of section 112.31446, Florida Statutes, is amended to read:

112.31446 Electronic filing system for financial disclosure.—

(6)~~(a) All secure login credentials held by the commission for the purpose of allowing access to the electronic filing system are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution.~~

~~(b)~~ Information entered in the electronic filing system for purposes of financial disclosure is exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution. Information entered in the electronic filing system is no longer exempt once the disclosure of financial interests or statement of financial interests is submitted to the commission or, in the case of a candidate, filed with a qualifying officer, whichever occurs first.

Section 7. Paragraph (g) of subsection (1) of section 119.07, Florida Statutes, is amended to read:

119.07 Inspection and copying of records; photographing public records; fees; exemptions.—

(1)

(g) In any civil action in which an exemption to this section is asserted, if the exemption is alleged to exist under or by virtue of s. 119.071(1)(d) ~~or (f)~~, (2)(d), (e), or (f), or (4)(c) or s. 119.0725(2)(h), the public record or part thereof in question shall be submitted to the court for an inspection in camera. If an exemption is alleged to exist under or by virtue of s. 119.071(2)(c), an inspection in camera is discretionary with the court. If the court finds that the asserted exemption is not applicable, it shall order the public record or part thereof in question to be immediately produced for inspection or copying as requested by the person seeking such access.

Section 8. Paragraph (f) of subsection (1) of section 119.071, Florida Statutes, is amended to read:

119.071 General exemptions from inspection or copying of public records.—

(1) AGENCY ADMINISTRATION.—

~~(f) Agency-produced data processing software that is sensitive is exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution. The designation of agency-produced software as sensitive does not prohibit an agency head from~~

~~sharing or exchanging such software with another public agency.~~

Section 9. Paragraph (f) of subsection (2) of section 119.0712, Florida Statutes, is amended to read:

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

(2) DEPARTMENT OF HIGHWAY SAFETY AND MOTOR VEHICLES.—

~~(f)1. Secure login credentials held by the Department of Highway Safety and Motor Vehicles are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution. This exemption applies to secure login credentials held by the department before, on, or after the effective date of the exemption. For purposes of this subparagraph, the term "secure login credentials" means information held by the department for purposes of authenticating a user logging into a user account on a computer, a computer system, a computer network, or an electronic device; an online user account accessible over the Internet, whether through a mobile device, a website, or any other electronic means; or information used for authentication or password recovery.~~

~~2. Internet protocol addresses, geolocation data, and other information held by the Department of Highway Safety and Motor Vehicles which 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, are exempt from s. 119.07(1) and s. 24(a),~~

~~Art. I of the State Constitution. This exemption applies to such information held by the department before, on, or after the effective date of the exemption. For purposes of this subparagraph, the term "public-facing portal" means a web portal or computer application accessible by the public over the Internet, whether through a mobile device, website, or other electronic means, which is established for administering chapter 319, chapter 320, chapter 322, chapter 328, or any other provision of law conferring duties upon 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, 2026, unless reviewed and saved from repeal through reenactment by the Legislature.~~

Section 10. Subsection (5) of section 119.0713, Florida Statutes, is amended to read:

119.0713 Local government agency exemptions from inspection or copying of public records.—

(5)~~(a)~~ Customer meter-derived data and billing information in increments less than one billing cycle ~~The following information~~ held by a utility owned or operated by a unit of local government is exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution.~~:~~

~~1. Information related to the security of the technology, processes, or practices of a utility owned or operated by a unit of local government that are designed to protect the utility's~~

~~networks, computers, programs, and data from attack, damage, or unauthorized access, which information, if disclosed, would facilitate the alteration, disclosure, or destruction of such data or information technology resources.~~

~~2. Information related to the security of existing or proposed information technology systems or industrial control technology systems of a utility owned or operated by a unit of local government, which, if disclosed, would facilitate unauthorized access to, and alteration or destruction of, such systems in a manner that would adversely impact the safe and reliable operation of the systems and the utility.~~

~~3. Customer meter-derived data and billing information in increments less than one billing cycle.~~

~~(b)~~ This exemption applies to such information held by a utility owned or operated by a unit of local government before, on, or after the effective date of this exemption.

~~(c)~~ This subsection is ~~Subparagraphs (a)1. and 2. are~~ subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2027, unless reviewed and saved from repeal through reenactment by the Legislature.

Section 11. Paragraph (b) of subsection (1) of section 119.0714, Florida Statutes, is amended to read:

119.0714 Court files; court records; official records.—

(1) COURT FILES.—Nothing in this chapter shall be

construed to exempt from s. 119.07(1) a public record that was made a part of a court file and that is not specifically closed by order of court, except:

(b) Data processing software as provided in s. 119.0725(2)(h) ~~s. 119.071(1)(f)~~.

Section 12. Subsection (10) of section 282.318, Florida Statutes, is renumbered as subsection (5), and paragraphs (d), (e), and (g) of subsection (4) and present subsections (5) through (9) of that section are amended, to read:

282.318 Cybersecurity.—

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

(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 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 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) 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.~~

~~(5) The portions of risk assessments, evaluations, external audits, and other reports of a state agency's cybersecurity program for the data, information, and information technology resources of the state agency which are held by a state agency are confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution if the disclosure of such portions of records would facilitate unauthorized access to or the unauthorized modification, disclosure, or destruction of:~~

~~(a) Data or information, whether physical or virtual; or~~

~~(b) Information technology resources, which include:~~

~~1. 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~~

~~2. Security information, whether physical or virtual, which relates to the agency's existing or proposed information technology systems.~~

~~For purposes of this subsection, "external audit" means an audit that is conducted by an entity other than the state agency that is the subject of the audit.~~

~~(6) Those portions of a public meeting as specified in s. 286.011 which would reveal records which are confidential and~~

~~exempt under subsection (5) are exempt from s. 286.011 and s. 24(b), Art. I of the State Constitution. No exempt portion of an exempt meeting may be off the record. All exempt portions of such meeting shall be recorded and transcribed. Such recordings and transcripts are confidential and exempt from disclosure under s. 119.07(1) and s. 24(a), Art. I of the State Constitution unless a court of competent jurisdiction, after an in camera review, determines that the meeting was not restricted to the discussion of data and information made confidential and exempt by this section. In the event of such a judicial determination, only that portion of the recording and transcript which reveals nonexempt data and information may be disclosed to a third party.~~

~~(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.~~

~~(8) The exemptions contained in subsections (5) and (6) apply to records held by a state agency before, on, or after the effective date of this exemption.~~

~~(9) Subsections (5) and (6) are subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2026, unless reviewed and saved from repeal through reenactment by the Legislature.~~

Section 13. Section 627.352, Florida Statutes, is repealed.

Section 14. Section 1004.055, Florida Statutes, is repealed.

Section 15. (1) The Legislature finds that it is a public necessity that the following information held by an agency be made confidential and exempt from s. 119.07(1), Florida Statutes, and s. 24(a), Article I of the State Constitution:

(a) Network schematics, hardware and software configurations, encryption information, or any information that identifies detection, investigation, or response practices relating to cybersecurity incidents, including breaches, if the disclosure of such information could facilitate unauthorized access to or unauthorized modification, disclosure, or destruction of data, information, or existing or proposed information technology or operational technology.

(b) Information relating to processes or practices designed to protect data, information, or existing or proposed information technology or operational technology if the disclosure of such information could facilitate unauthorized access to or unauthorized modification, disclosure, or

destruction of such data, information, or technology.

(c) Portions of risk assessments, evaluations, audits, and other reports of an agency's cybersecurity program if the disclosure of such information could facilitate unauthorized access to or unauthorized modification, disclosure, or destruction of data, information, or existing or proposed information technology or operational technology.

(d) Login credentials.

(e) 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.

(f) Agency-produced data processing software that is sensitive.

(g) Insurance and self-insurance coverage limits and deductibles, as well as any other risk mitigation coverages, acquired for the protection of information technology, operational technology, or data of an agency.

Release of such information could place an agency at greater risk of breaches, cybersecurity incidents, and ransomware attacks. Network schematics, hardware and software configurations, encryption information, or any information that identifies detection, investigation, or response practices for

cybersecurity incidents, including breaches reveal how an agency's information technology and operational technology systems are structured and defended. Disclosure of such information could enable a malicious actor to map system architecture, identify vulnerabilities, and bypass security controls. Information describing processes or practices designed to protect data, information, or existing or proposed information technology or operational technology could similarly be used to exploit weaknesses and predict defensive actions. Portions of risk assessments, evaluations, audits, and other reports of an agency's cybersecurity program routinely include descriptions of vulnerabilities, testing results, and recommendations. Disclosure of such information would substantially increase the likelihood of a successful cyberattack. Login credentials are a foundational security control and disclosure of such information could allow malicious actors to authenticate into government systems, impersonate legitimate users, and access personal identifying and other sensitive information. Internet protocol addresses, geolocation data, and other information which 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 could be used to track usage patterns, identify remote access points, or monitor portal vulnerabilities. Sensitive agency-produced data processing

software can reveal the inner workings of security controls, authentication mechanisms, or automated processes that malicious actors can use to exploit weaknesses in security measures. If information related to coverage limits and deductibles of cybersecurity insurance were disclosed, it could give cybercriminals an understanding of the monetary sum an agency can afford or may be willing to pay as a result of a ransomware attack at the expense of the taxpayer. Accordingly, the Legislature finds that the disclosure of such sensitive cybersecurity-related information would significantly impair the administration of vital governmental programs.

(2) The Legislature also finds that it is a public necessity that any portion of a meeting that would reveal the confidential and exempt information by made exempt from s. 286.011, Florida Statutes, and s. 24(b), Article I of the State Constitution, and that any recordings and transcripts of the closed portion of a meeting be made confidential and exempt from s. 119.07(1), Florida Statutes, and s. 24(a), Article I of the State Constitution. The 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.

(3) For these reasons, the Legislature finds that these public records and public meetings exemptions are of the utmost importance and are a public necessity.

Section 16. This act shall take effect upon becoming a law.