FOR CONSIDERATION By the Committee on Appropriations

576-02763A-23 20232508pb

A bill to be entitled

An act relating to state cybersecurity operations; providing for a type two transfer of the Cybersecurity Operations Center and related services, including the position of the state chief information security officer, from the Florida Digital Service within the Department of Management Services to the Department of Law Enforcement; amending s. 282.318, F.S.; requiring the Department of Management Services, acting through the Florida Digital Service, to perform specified actions relating to state agency cybersecurity risks; requiring the Department of Management Services to perform specified actions in consultation with and with approval from the state chief information security officer; requiring that the cybersecurity governance framework minimum guidelines be consistent with the state cybersecurity strategic plan; specifying that the Department of Law Enforcement is the lead entity responsible for enterprise cybersecurity operations; requiring the Department of Law Enforcement to designate a state chief information security officer; providing the qualifications for and the responsibilities of the state chief information security officer; requiring that the state chief information security officer be notified of all confirmed or suspected incidents involving, or threats to, state agency information; requiring the state chief information security officer to report such incidents to the Governor and the state chief

information officer; requiring the Department of Law Enforcement to develop, and annually update by a specified date, a certain state cybersecurity strategic plan; requiring the Department of Law Enforcement to operate and maintain the Cybersecurity Operations Center as part of the Florida Fusion Center; requiring that the center be staffed with specified personnel; requiring the center to coordinate with the Florida Digital Service to support state agencies and their responses to cybersecurity incidents; requiring the Department of Law Enforcement to review and approve, before publication, the cybersecurity governance framework established by the Florida Digital Service; requiring the Department of Law Enforcement to review and approve all cybersecurity training provided by or facilitated through the Florida Digital Service; requiring the Department of Law Enforcement to develop and publish specified guidelines and processes for establishing a cybersecurity incident reporting process for use by state agencies; requiring the Florida Digital Service to provide certain reports on a periodic basis to the Legislature, the state chief information security officer, and the Cybersecurity Advisory Council; prohibiting the report transmitted to the advisory council from containing certain information; requiring state agency heads, in consultation with the Cybersecurity Operations Center, the Cybercrime Office, and the Florida Digital Service, to establish

an agency cybersecurity response team to respond to cybersecurity incidents; requiring state agencies to submit a corrective action plan to the Florida Digital Service within a specified timeframe for all findings confirmed by the state chief information security officer; requiring that certain implementation plans be submitted to the state chief information officer on a periodic basis; requiring that a specified comprehensive risk assessment be conducted annually; providing that certain public records exemptions do not apply to information made available to the Cybersecurity Operations Center; providing that certain mandatory cybersecurity awareness training offered to state employees may be provided in collaboration with the Cyber Security Operations Center or the Florida Digital Service; conforming a provision to changes made by the act; requiring state agency heads to submit after-action reports to the Department of Law Enforcement and other specified entities; requiring that certain confidential and exempt records be made available to the state chief information officer; requiring the Department of Law Enforcement to adopt specified rules; amending s. 282.3185, F.S.; requiring that certain cybersecurity training programs developed by the Florida Digital Service be approved by the state chief information security officer; authorizing the Florida Digital service to collaborate with the Cybersecurity Operations Center to provide certain cybersecurity

training; requiring local governments to provide notification of a cybersecurity or ransomware incident to the Florida Digital Service and other entities within a specified timeframe after the incident; requiring local governments to provide a certain report of cybersecurity incidents or ransomware incidents of a specified severity level to the Florida Digital Service and other entities; authorizing local governments to provide a certain report of cybersecurity incidents or ransomware incidents of a specified severity level to the Florida Digital Service; requiring the Florida Digital Service to provide certain consolidated incident reports to the state chief information security officer and other entities; requiring the Florida Digital Service to collaborate with the state chief information security officer to establish guidelines and processes for submitting after-action reports, by a specified date; conforming a cross-reference; providing an effective date.

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

Section 1. All positions, duties, functions, records, existing contracts, administrative authority, administrative rules, and unexpended balances of appropriations, allocations, and other public funds relating to the Cybersecurity Operations Center and related services, including the position of the state chief information security officer, of the Florida Digital

Service within the Department of Management Services are transferred by a type two transfer as defined in s. 20.06(2), Florida Statutes, to the Department of Law Enforcement.

Section 2. Section 282.318, Florida Statutes, is amended to read:

282.318 Cybersecurity.—

(1) This section may be cited as the "State Cybersecurity Act."

(2) As used in this section, the term "state agency" has the same meaning as provided in s. 282.0041, except that the term includes the Department of Legal Affairs, the Department of Agriculture and Consumer Services, and the Department of Financial Services.

(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 for cybersecurity, including the National Institute for Standards and Technology Cybersecurity Framework~~, for cybersecurity~~. The department, acting through the Florida Digital Service, shall:

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

(b) Annually review the strategic and operational cybersecurity plans of state agencies for compliance with the cybersecurity governance framework. The review of the plans must include the following:

1. Providing findings to the state chief information security officer for review and confirmation;

2. Notifying agencies of confirmed findings and the date by which the agency must submit a corrective action plan;

3. Reviewing corrective action plans submitted by agencies;

4. Tracking and monitoring progress of the implementation of corrective action plans; and

5. Annually submitting a report to the state chief information security officer which includes, by agency, completed reviews, any confirmed findings, a brief description of corresponding corrective action plans, and the status of corrective action plan implementation.

(c) Review state agency annual risk assessment findings and corresponding remediation plans, including:

1. Tracking and monitoring the progress of the risk assessment remediation plans; and

2. Annually submitting a report to the state chief information security officer which includes, by agency, risk assessment findings, a brief description of corresponding remediation plans, and the status of remediation plan implementation.

(d) Annually provide cybersecurity training for state agency information security managers and computer security incident response team members which includes training on cybersecurity threats, trends, and best practices. The training curriculum must be approved by the state chief information security officer.

(e) 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 subparagraph (5)(g)1. The training must be approved by the state chief information security officer and may be provided in collaboration with a private sector entity or an institution of the State University System.

(4) The department, acting through the Florida Digital Service, and in consultation with and with approval from the state chief information security officer, shall:

(a) 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.~~

(b) ~~(c)~~ Develop and publish for use by state agencies a cybersecurity governance framework consistent with the state cybersecurity strategic plan which ~~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.~~

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

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

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

6.~~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.

7.~~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 incident determined by the state agency to be of severity level 3, 4, or 5 to the Cybersecurity Operations Center and the Cybercrime Office of the Department of Law Enforcement as soon as possible but no later than 48 hours after discovery of the cybersecurity incident and no later than 12 hours after discovery of the ransomware incident. The report must contain the information required in sub-subparagraph b.~~

~~(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.~~

~~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).~~

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

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

10.~~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.

11.~~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.

12.~~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, 2023 ~~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.~~

(5) The Department of Law Enforcement is the lead entity responsible for enterprise cybersecurity operations and as the lead entity, the Department of Law Enforcement shall:

(a) Designate an employee 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 must be notified of all confirmed or suspected incidents involving, or threats to, state agency information technology resources and must report such incidents or threats to the Governor and the state chief information officer.

(b) Develop, and annually update by February 1, a state 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) ~~(h)~~ Operate and maintain a Cybersecurity Operations Center as part of the Florida Fusion 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 Florida Digital Service ~~Department of Law Enforcement~~

to support state agencies and their response to any confirmed or suspected cybersecurity incident.

(d) Before publication, review and approve the cybersecurity governance framework established by the Florida Digital Service.

(e) Review and approve all cybersecurity training provided by or facilitated through the Florida Digital Service within the Department of Management Services.

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

(g) Develop and publish for use by state agencies guidelines and processes for establishing a cybersecurity incident reporting process that includes procedures and secure communication mechanisms for notifying the Department of Law Enforcement, the Florida Digital Service, and other stakeholders of cybersecurity incidents.

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

a. Level 5 is an emergency-level incident within the specified jurisdiction which 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.

b. 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.

c. 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.

d. 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.

e. 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.

2. 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 information must, at a minimum, include all of the following:

a. A summary of the facts surrounding the cybersecurity incident or ransomware incident.

b. 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 whether the backup was created using cloud computing.

c. The types of data compromised by the cybersecurity incident or ransomware incident.

d. The estimated fiscal impact of the cybersecurity incident or ransomware incident.

e. In the case of a ransomware incident, the details of the ransom demanded.

3.a. A state agency shall report all ransomware incidents and any cybersecurity incident determined by the state agency to

be of severity level 3, 4, or 5 to the Cybersecurity Operations Center, the Cybercrime Office within the Department of Law Enforcement, and the Florida Digital Service as soon as possible but no later than 48 hours after discovery of the cybersecurity incident and no later than 12 hours after discovery of the ransomware incident. The report must contain the information required to be reported under subparagraph 2.

b. 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.

4. 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, the Cybercrime Office within the Florida Department of Law Enforcement, and the Florida Digital Service as soon as possible. The report must contain the information required to be reported under subparagraph 2.

5. The Florida Digital Service shall provide a consolidated incident report on a quarterly basis to the President of the Senate, the Speaker of the House of Representatives, the state chief information security officer, 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).

(6) ~~(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 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 Cybersecurity Operations Center ~~department, through the Florida Digital Service,~~ and the Cybercrime Office within ~~of~~ the Department of Law Enforcement and the Florida Digital Service within the Department of Management Services, 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 (5)(g) ~~(3)(c)~~.

(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 of Law Enforcement 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.

3. State agencies must submit a corrective action plan for all findings confirmed by the state chief information security officer to the Florida Digital Service within 90 days after notifications. Implementation plans that report the status of the corrective action plans must be submitted on a quarterly basis to the state chief information officer until fully implemented.

(d) Annually 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 must ~~shall~~ be available to the Auditor General, the Florida Digital Service within the department, the Cybercrime Office and the

Cybersecurity Operations Center within ~~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 and the Cybersecurity Operations Center within ~~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 must ~~shall~~ be available to the Auditor General, the Cybercrime Office and the Cybersecurity Operations Center within ~~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 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 must ~~shall~~ be available to the Auditor General, the Cybercrime Office and the Cybersecurity Operations Center within ~~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 and the Cybersecurity Operations Center within ~~of~~ the Department of Law Enforcement, the Florida Digital Service, 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 of Law Enforcement ~~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 (5)(g) ~~(3)(c)~~.

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

(k) Submit to the Department of Law Enforcement and 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)~~(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.

(8) ~~(6)~~ Those portions of a public meeting as specified in s. 286.011 which would reveal records which are confidential and exempt under subsection (7) ~~(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 must ~~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.

(9) ~~(7)~~ The portions of records made confidential and exempt in subsections (7) ~~(5)~~ and (8) must ~~(6) shall~~ be available to

the Auditor General, the Cybercrime Office and the state chief information officer within ~~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)~~(8)~~ The exemptions contained in subsections (7) ~~(5)~~ and (8) ~~(6)~~ apply to records held by a state agency before, on, or after the effective date of this exemption.

(11)~~(9)~~ Subsections (7) ~~(5)~~ and (8) ~~(6)~~ are subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2025, unless reviewed and saved from repeal through reenactment by the Legislature.

(12)~~(10)~~ The department and the Department of Law Enforcement shall adopt rules relating to cybersecurity and to administer this section.

Section 3. Section 282.3185, Florida Statutes, is amended to read:

282.3185 Local government cybersecurity.—

(1) SHORT TITLE.—This section may be cited as the "Local Government Cybersecurity Act."

(2) DEFINITION.—As used in this section, the term "local government" means any county or municipality.

(3) CYBERSECURITY TRAINING.—

(a) The Florida Digital Service shall:

1. Develop a basic cybersecurity training curriculum for local government employees which must be approved by the state

chief information security officer. All local government employees with access to the local government's network must complete the basic cybersecurity training within 30 days after commencing employment and annually thereafter.

2. Develop an advanced cybersecurity training curriculum for local governments which is consistent with the cybersecurity training required under s. 282.318(3)(e) and which must be approved by the state chief information security officer ~~s. 282.318(3)(g)~~. All local government technology professionals and employees with access to highly sensitive information must complete the advanced cybersecurity training within 30 days after commencing employment and annually thereafter.

(b) The Florida Digital Service may provide the cybersecurity training required by this subsection in collaboration with the Cybercrime Office and the Cybersecurity Operations Center within ~~of~~ the Department of Law Enforcement, a private sector entity, or an institution of the State University System.

(4) CYBERSECURITY STANDARDS.—

(a) Each local government shall adopt cybersecurity standards that safeguard its data, information technology, and information technology resources to ensure availability, confidentiality, and integrity. The cybersecurity standards must be consistent with generally accepted best practices for cybersecurity, including the National Institute of Standards and Technology Cybersecurity Framework.

(b) Each county with a population of 75,000 or more must adopt the cybersecurity standards required by this subsection by January 1, 2024. Each county with a population of less than

75,000 must adopt the cybersecurity standards required by this subsection by January 1, 2025.

(c) Each municipality with a population of 25,000 or more must adopt the cybersecurity standards required by this subsection by January 1, 2024. Each municipality with a population of less than 25,000 must adopt the cybersecurity standards required by this subsection by January 1, 2025.

(d) Each local government shall notify the Florida Digital Service of its compliance with this subsection as soon as possible.

(5) INCIDENT NOTIFICATION.—

(a) A local government shall provide notification of a cybersecurity incident or ransomware incident to the Cybersecurity Operations Center and the~~,~~ Cybercrime Office within ~~of~~ the Department of Law Enforcement, the Florida Digital Service, and the sheriff who has jurisdiction over the local government in accordance with paragraph (b). The notification must include, at a minimum, the following information:

1. A summary of the facts surrounding the cybersecurity incident or ransomware incident.

2. The date on which the 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.

3. The types of data compromised by the cybersecurity incident or ransomware incident.

4. The estimated fiscal impact of the cybersecurity incident or ransomware incident.

5. In the case of a ransomware incident, the details of the

ransom demanded.

6. A statement requesting or declining assistance from the Cybersecurity Operations Center and~~,~~ the Cybercrime Office within ~~of~~ the Department of Law Enforcement, the Florida Digital Service, or the sheriff who has jurisdiction over the local government.

(b)1. A local government shall report all ransomware incidents and any cybersecurity incident determined by the local government to be of severity level 3, 4, or 5 as provided in s. 282.318(5)(g) ~~s. 282.318(3)(c)~~ to the Cybersecurity Operations Center and~~,~~ the Cybercrime Office within ~~of~~ the Department of Law Enforcement, the Florida Digital Service, and the sheriff who has jurisdiction over the local government as soon as possible but no later than 48 hours after discovery of the cybersecurity incident and no later than 12 hours after discovery of the ransomware incident. The report must contain the information required in paragraph (a).

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.

(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(5)(g) ~~s. 282.318(3)(c)~~ to the Cybersecurity Operations Center and~~,~~ the Cybercrime Office within ~~of~~ the Department of Law Enforcement, the Florida Digital

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

(d) The Florida Digital Service ~~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, the state chief information security officer, and the Florida Cybersecurity Advisory Council. The report provided to the Florida Cybersecurity Advisory Council may not contain the name of any local government, 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).

(6) AFTER-ACTION REPORT.—A local government must submit to the Cybersecurity Operations Center and 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. By December 1, 2023 ~~2022~~, the Florida Digital Service shall collaborate with the state chief information security officer to establish guidelines and processes for submitting an after-action report.

Section 4. This act shall take effect July 1, 2023.