A bill to be entitled

An act relating to cybersecurity; amending s. 252.351, F.S.; requiring a list of reportable incidents maintained by the Division of Emergency Management to include cybersecurity incidents and ransomware incidents; requiring a political subdivision to report cybersecurity incidents and ransomware incidents to the State Watch Office; amending s. 282.0041, F.S.; providing definitions; amending s. 282.318, F.S.; requiring the Department of Management Services, acting through the Florida Digital Service, to develop and publish guidelines and processes for reporting cybersecurity incidents to certain entities; requiring a state agency to report certain information following a cybersecurity or ransomware incident; requiring the department, acting through the Florida Digital Service, to develop and publish guidelines for the submission of after-action reports, provide annual cybersecurity training to certain persons, and provide after-action reports to the Florida Cybersecurity Advisory Council on a monthly basis; requiring state agency heads to annually provide cybersecurity awareness training to certain persons and report cybersecurity incidents, ransomware incidents, and cybersecurity breaches to specified entities;

requiring ransomware incidents to be reported within a certain period; requiring state agency heads to submit certain after-action reports to the Florida Digital Service; creating s. 282.3185, F.S.; providing a short title; providing a definition; requiring the Florida Digital Service to develop certain cybersecurity training curriculum; requiring certain persons to complete certain training within a specified period and annually thereafter; authorizing the Florida Digital Service to provide certain training in collaboration with certain entities; requiring certain local governments to adopt certain cybersecurity standards by specified dates; requiring a local government to provide certain notification to the Florida Digital Service; requiring a local government to notify the State Watch Office and sheriff of a cybersecurity incident or ransomware incident; providing notification requirements; requiring the office to immediately forward certain information to the Cybersecurity Operations Center and the Cybercrime Office of the Department of Law Enforcement; authorizing the Cybersecurity Operations Center and the Cybercrime Office to provide certain support to a local government; requiring the Cybersecurity Operations Center to provide certain information to

the Florida Cybersecurity Advisory Council; requiring a local government to submit to the Florida Digital Service an after-action report containing certain information; requiring the Florida Digital Service to provide after-action reports to the council on a monthly basis; requiring the Florida Digital Service to establish certain guidelines by a specified date; creating s. 282.3186, F.S.; prohibiting certain entities from paying or otherwise complying with a ransom demand; amending s. 282.319, F.S.; revising the purpose of the Florida Cybersecurity Advisory Council to include advising counties and municipalities on cybersecurity; requiring the council to meet at least quarterly to review certain information and develop and make certain recommendations; requiring the council to annually submit to the Governor and the Legislature a certain ransomware incident report beginning on a specified date; providing requirements for the report; providing a definition; creating s. 815.062, F.S.; providing a definition; providing criminal penalties; requiring a person convicted of certain offenses to pay a certain fine; requiring deposit of certain moneys in the General Revenue Fund; providing a legislative finding and declaration of an important state interest; providing an effective date.

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

Section 1. Subsection (3) of section 252.351, Florida Statutes, is amended, and paragraphs (l) and (m) are added to subsection (2) of that section, to read:

252.351 Mandatory reporting of certain incidents by political subdivisions.—

(2) The division shall create and maintain a list of reportable incidents. The list shall include, but is not limited to, the following events:

(l) Cybersecurity incidents as those terms are defined in s. 282.0041.

(m) Ransomware incidents as defined in s. 282.0041.

(3)(a) As soon as practicable following its initial response to an incident, a political subdivision shall provide notification to the office that an incident specified on the list of reportable incidents has occurred within its geographical boundaries.

(b) The division may establish guidelines specifying the method and format a political subdivision must use when reporting an incident.

(c) A political subdivision must report a cybersecurity incident or ransomware incident to the office pursuant to s. 282.3185.

Section 2. Subsections (24) through (27) and (28) through (37) of section 282.0041, Florida Statutes, are renumbered as subsections (25) through (28) and (30) through (39), respectively, and new subsections (24) and (29) are added to that section to read:

282.0041 Definitions.—As used in this chapter, the term:

(24) "Office" means the State Watch Office established within the Division of Emergency Management pursuant to s. 14.2016.

(29) "Ransomware incident" means a malicious cybersecurity incident in which a person or entity introduces software that encrypts, modifies, or otherwise renders unavailable a state agency's, county's, or municipality's data and thereafter the person or entity demands a ransom to restore access to the data or otherwise remediate the impact of the software.

Section 3. Paragraphs (c) and (g) of subsection (3) and paragraphs (i) and (j) of subsection (4) of section 282.318, Florida Statutes, are amended, and paragraph (j) is added to subsection (3) and paragraph (k) is added to subsection (4) of that section, to read:

282.318 Cybersecurity.—

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

(c) Develop and publish for use by state agencies a cybersecurity governance framework 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.

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

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

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

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.

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 and tiered reporting timeframes for notifying the department, ~~and~~ the Department of Law Enforcement, the President of the Senate, and the Speaker of the House of Representatives of cybersecurity incidents. The tiered reporting timeframes shall be based upon the level of severity of the cybersecurity incidents being reported. The cybersecurity incident reporting process shall 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:

a. A summary of the events 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, 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 ransom demanded.

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

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

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.

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.

14. Submitting after-action reports following a cybersecurity incident or ransomware incident pursuant to subsection (4).

(g) Annually provide cybersecurity training to all state agency technology professionals and employees with access to highly sensitive information which ~~that~~ develops, assesses, and documents competencies by role and skill level. 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.

(j) Provide any after-action reports received pursuant to this section to the Florida Cybersecurity Advisory Council on a monthly basis.

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

(i) Provide cybersecurity awareness training to all state agency employees within ~~in the first~~ 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 of the Department of Law Enforcement, 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 through the Florida Digital Service.

1. All cybersecurity incidents, ransomware incidents, and breaches must be reported by state agencies to the Florida Digital Service within the department, ~~and~~ the Cybercrime Office of the Department of Law Enforcement, the President of the Senate, and the Speaker of the House of Representatives and such reports must comply with the notification procedures and reporting timeframes established pursuant to paragraph (3)(c). However, a ransomware incident must be reported within 12 hours after the state agency discovers the incident.

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

(k) Submit to the Florida Digital Service at the conclusion 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.

Section 4. Section 282.3185, Florida Statutes, is created 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.—The Florida Digital Service:

(a) Shall develop a basic cybersecurity practices training curriculum for local government employees. 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.

(b) Shall develop an advanced cybersecurity training curriculum for local governments which is consistent with the cybersecurity training required under 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.

(c) May provide the cybersecurity training required by this subsection in collaboration with the Cybercrime Office 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 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 fewer 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 fewer 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 practicable.

(5) INCIDENT NOTIFICATION.—

(a) A local government shall provide notification of a cybersecurity incident or ransomware incident to the office pursuant to s. 252.351 and to the sheriff who has jurisdiction over the local government. The notification must include, at a minimum, the following information:

1. A summary of the events 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, and whether 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 ransom demanded.

(b) Notification must be provided as soon as practicable but no later than:

1. Forty-eight hours after a local government discovers a cybersecurity incident.

2. Twelve hours after a local government discovers a ransomware incident.

(c) The office shall immediately forward all cybersecurity incident and ransomware incident information to the Cybersecurity Operations Center operated and maintained pursuant to s. 282.318(3)(h) and the Cybercrime Office of the Department of Law Enforcement. The Cybersecurity Operations Center and the Cybercrime Office shall review the reported information and may provide support to the local government in its response to the cybersecurity incident or ransomware incident. The Cybersecurity Operations Center shall provide all information received relating to the cybersecurity incident or ransomware incident to the Florida Cybersecurity Advisory Council.

(6) AFTER-ACTION REPORT.—After a cybersecurity incident or ransomware incident has concluded, the reporting local government shall submit an after-action report to the Florida Digital Service that summarizes the incident, the incident's resolution, and any insights gained as a result of the incident. The Florida Digital Service shall provide all after-action reports to the Florida Cybersecurity Advisory Council on a monthly basis. By December 1, 2022, the Florida Digital Service shall establish guidelines specifying the method and format for submitting an after-action report.

Section 5. Section 282.3186, Florida Statutes, is created to read:

282.3186 Ransomware incident compliance.—A state agency as defined in s. 282.318(2), a county, or a municipality experiencing a ransomware incident may not pay or otherwise comply with a ransom demand.

Section 6. Subsections (2) of section 282.319, Florida Statutes, is amended, paragraphs (g) and (h) are added to subsection (9), and subsections (12) and (13) are added to that section, to read:

282.319 Florida Cybersecurity Advisory Council.—

(2) The purpose of the council is to:

(a) Assist state agencies in protecting their information technology resources from cybersecurity ~~cyber~~ threats and incidents.

(b) Advise counties and municipalities on cybersecurity, including cybersecurity threats, trends, and best practices.

(9) The council shall meet at least quarterly to:

(g) Review information relating to cybersecurity incidents and ransomware incidents to determine commonalities and develop best practice recommendations for state agencies, counties, and municipalities.

(h) Recommend any additional information that a county or municipality should report to the office as part of its cybersecurity incident or ransomware incident notification pursuant to ss. 252.351 and 282.3185.

(12) Beginning December 1, 2022, and each December 1 thereafter, the council shall submit to the Governor, the President of the Senate, and the Speaker of the House of Representatives a comprehensive report that includes data, trends, analysis, findings, and recommendations for state and local action regarding ransomware incidents. At a minimum, the report must include:

(a) Descriptive statistics including the amount of ransom requested, duration of the incident, and overall monetary cost to taxpayers of the incident.

(b) A detailed statistical analysis of the circumstances that led to the ransomware incident, including breadth of employee training and frequency of data backup.

(c) Specific issues identified with current policies,

procedures, rules, or statutes and recommendations to address such issues.

(d) Any other recommendations to prevent ransomware incidents.

(13) For purposes of this section, the term "state agency" has the same meaning as provided in s. 282.318(2).

Section 7. Section 815.062, Florida Statutes, is created to read:

815.062 Offenses against governmental entities.—

(1) As used in this section the term "governmental entity" means any official, officer, commission, board, authority, council, committee, or department of the executive, judicial, or legislative branch of state government; any state university; and any county or municipality, special district, water management district, or other political subdivision of the state.

(2) A person who willfully, knowingly, and without authorization introduces a computer contaminant that encrypts, modifies, or otherwise renders unavailable data, programs, or supporting documentation residing or existing within a computer, computer system, computer network, or electronic device owned or operated by a governmental entity and demands a ransom to restore access to the data, programs, or supporting documentation or otherwise remediate the impact of the computer contaminant commits a felony of the first degree, punishable as

provided in s. 775.082, s. 775.083, or s. 775.084.

(3) An employee or contractor of a governmental entity with access to the governmental entity's network who willfully and knowingly aids or abets another in the commission of a violation of subsection (2) commits a felony of the first degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(4) In addition to any other penalty imposed, a person convicted of a violation of this section must pay a fine equal to twice the amount of the ransom demand. Moneys recovered under this subsection shall be deposited into the General Revenue Fund.

Section 8. The Legislature finds and declares that this act fulfills an important state interest.

Section 9. This act shall take effect July 1, 2022.