An act relating to cybersecurity; amending s. 282.0041, F.S.; providing and revising 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; requiring state agencies to report ransomware incidents and certain cybersecurity incidents to certain entities within specified timeframes; requiring the Cybersecurity Operations Center to provide certain notifications to the Legislature within a specified timeframe; requiring the Cybersecurity Operations Center to quarterly provide certain reports to the Legislature and the Florida Cybersecurity Advisory Council; requiring the department, acting through the Florida Digital Service, to develop and publish guidelines and processes by a specified date for submitting after-action reports and annually provide cybersecurity training to certain persons; requiring state agency heads to annually provide cybersecurity awareness training to certain persons; requiring state agencies to report cybersecurity incidents and ransomware incidents in compliance with certain procedures and timeframes; requiring state agency heads to submit certain after-action reports to the Florida Digital Service within a specified timeframe; creating s. 282.3185, F.S.; providing a short title; providing a definition; requiring the Florida Digital Service to develop certain cybersecurity training curricula; requiring certain persons to complete certain cybersecurity training within a specified timeframe 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 local governments to provide certain notification to the Florida Digital Service and certain entities; providing notification requirements; requiring local governments to report ransomware incidents and certain cybersecurity incidents to certain entities within specified timeframes; requiring the Cybersecurity Operations Center to provide certain notification to the Legislature within a specified timeframe; authorizing local governments to report certain cybersecurity incidents to certain entities; requiring the Cybersecurity Operations Center to quarterly provide certain reports to the Legislature and the

Florida Cybersecurity Advisory Council; requiring local governments to submit after-action reports containing certain information to the Florida Digital Service within a specified timeframe; requiring the Florida Digital Service to establish certain guidelines and processes 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. Subsections (28) through (37) of section 282.0041, Florida Statutes, are renumbered as subsections (29) through (38), respectively, subsection (19) is amended, and a new subsection (28) is added to that section, to read:

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

(19) "Incident" means a violation or imminent threat of violation, whether such violation is accidental or deliberate, of information technology resources, security, policies, or practices. An imminent threat of violation refers to a situation in which a ~~the~~ state agency, county, or municipality has a factual basis for believing that a specific incident is about to occur.

(28) "Ransomware incident" means a malicious cybersecurity incident in which a person or entity introduces software that gains unauthorized access to or 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 prevent the publication of the data, restore access to the data, or otherwise remediate the impact of the software.

Section 2. 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 (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 of cybersecurity incidents. ~~The tiered reporting timeframes~~

~~shall be based upon the level of severity of the cybersecurity incidents being reported.~~

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).

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. Such guidelines and processes for submitting after-action reports must be developed and published by December 1, 2022.

(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 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.

(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 and ransomware incidents ~~breaches~~ must be reported by state agencies. Such reports ~~to the Florida Digital Service within the department and the Cybercrime Office of the Department of Law Enforcement and~~ must comply with the notification procedures and reporting timeframes established pursuant to paragraph (3)(c).

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

(k) Submit to 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.

Section 3. 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.—

(a) The Florida Digital Service shall:

1. Develop a basic cybersecurity 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.

2. 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.

(b) The Florida Digital Service 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 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, Cybercrime Office of the Department of Law Enforcement, and 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, the Cybercrime Office of the Department of Law Enforcement, 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(3)(c) to the Cybersecurity Operations Center, the Cybercrime Office of the Department of Law Enforcement, 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(3)(c) to the Cybersecurity Operations Center, the Cybercrime Office of the Department of Law Enforcement, and the sheriff who has jurisdiction over the local government. The report shall contain the information required in paragraph (a).

(d) 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 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 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, 2022, the Florida Digital Service shall establish guidelines and processes for submitting an after-action report.

Section 4. 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 5. 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 Florida Digital Service as part of its cybersecurity incident or ransomware incident notification pursuant to s. 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 ransomware incident, and overall monetary cost to taxpayers of the ransomware incident.

(b) A detailed statistical analysis of the circumstances that led to the ransomware incident which does not include the name of the state agency, county, or municipality; network information; or system identifying information.

(c) A detailed statistical analysis of the level of cybersecurity employee training and frequency of data backup for the state agency, county, or municipality that reported the ransomware incident.

(d) Specific issues identified with current policies, procedures, rules, or statutes and recommendations to address such issues.

(e) 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 6. 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; or 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 gains unauthorized access to, 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 prevent the publication of or restore access to the data, programs, or supporting documentation or to 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 7. The Legislature finds and declares that this act fulfills an important state interest.

Section 8. This act shall take effect July 1, 2022.