By Senator Hutson

7-01444A-22 20221670__

A bill to be entitled

An act relating to cybersecurity; amending s. 252.351, F.S.; requiring specified entities to report certain computer attacks to the State Watch Office within the Division of Emergency Management; creating s. 282.3185, F.S.; defining terms; requiring local governments to adopt certain cybersecurity standards by a specified date; requiring local governments to report certain information to the Florida Digital Service; requiring local governments to conduct vulnerability testing at certain intervals; requiring certain local government employees and persons to undergo specified training; requiring the Florida Digital Service and the Florida Cybersecurity Advisory Council to develop training requirements and conduct training at certain intervals; requiring state agencies and local governments to report certain incidents to specified entities within specified time periods; requiring a report on certain incidents to be submitted to the Florida Cybersecurity Advisory Council; prohibiting local governments from paying a ransom before communicating with specified entities; requiring the Florida Digital Service to create a specified checklist; amending s. 815.06, F.S.; defining the term "ransomware"; prohibiting specified offenses concerning ransomware; providing criminal penalties; providing for disposition of fines for such offenses; providing an appropriation; providing an effective date.

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

Section 1. Subsection (2) of section 252.351, Florida Statutes, is amended, 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:

(a) Major fires, including wildfires, commercial or multiunit residential fires, or industrial fires.

(b) Search and rescue operations, including structure collapses or urban search and rescue responses.

(c) Bomb threats or threats to inflict harm on a large number of people or significant infrastructure, suspicious devices, or device detonations.

(d) Natural hazards and severe weather, including earthquakes, landslides, or ground subsidence or sinkholes.

(e) Public health and population protective actions, including public health hazards, evacuation orders, or emergency shelter openings.

(f) Animal or agricultural events, including suspected or confirmed animal diseases, suspected or confirmed agricultural diseases, crop failures, or food supply contamination.

(g) Environmental concerns, including an incident of reportable pollution release as required in s. 403.077(2).

(h) Nuclear power plant events, including events in process or that have occurred which indicate a potential degradation of

the level of safety of the plant or which indicate a security threat to facility protection.

(i) Major transportation events, including aircraft or airport incidents, passenger or commercial railroad incidents, major road or bridge closures, or marine incidents involving a blocked navigable channel of a major waterway.

(j) Major utility or infrastructure events, including dam failures or overtopping, drinking water facility breaches, or major utility outages or disruptions involving transmission lines or substations.

(k) Military events, when information regarding such activities is provided to a political subdivision.

(l) Attacks on a computer or network of a local government, as defined in s. 215.89(2)(c), or a hospital, as defined in s. 395.002(13), including ransomware attacks and data breaches.

Section 2. Section 282.3185, Florida Statutes, is created to read:

282.3185 Local governments; cybersecurity.—

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

(a) "Local government" has the same meaning as provided in s. 215.89(2)(c).

(b) "Ransomware" has the same meaning as provided in s. 815.06(1).

(2)(a) By January 1, 2024, each local government must adopt cybersecurity standards for all information technology and operational technology which comply with the National Institute of Standards and Technology cybersecurity framework that is appropriate for the size of the organization. Redundancies such as routine backups of critical information and multifactor

authentication must be required as part of these standards. A local government shall report its standards to the Florida Digital Service.

(b) Each local government must conduct vulnerability testing of its information technology and operational technology not less than every 2 years.

(3)(a) Each local government employee with access to a local government network must receive training when he or she begins employment and at intervals thereafter, as specified by the Florida Digital Service which, at a minimum, addresses phishing and digital hygiene.

(b) All local government technology professionals and persons with access to highly sensitive information shall be required to undergo intensive cybersecurity training.

(c) The Florida Digital Service and the Florida Cybersecurity Advisory Council shall develop the training requirements and conduct each training virtually at certain times of the year.

(4) All state agencies, as defined in s. 282.602(6), and local governments shall report all cybersecurity and ransomware incidents to the State Watch Office, the Florida Digital Service, the Executive Office of the Governor, the Department of Law Enforcement, and local law enforcement agencies within 12 hours of discovery. The state chief information officer and the Florida Cybersecurity Advisory Council will directly advise the Governor on the event. Once a cybersecurity or ransomware incident has concluded, a report must be submitted to the Florida Cybersecurity Advisory Council which summarizes the incident, how the incident was resolved, and lessons learned.

(5)(a) If a ransomware incident or cyber extortion incident has occurred, a local government may not pay ransom before communicating with the Florida Digital Service and the local law enforcement agencies.

(b) The Florida Digital Service shall create a ransomware checklist for local governments which lists the factors a local government must consider before paying a ransom.

Section 3. Present subsections (5) through (9) of section 815.06, Florida Statutes, are redesignated as subsections (6) through (10), respectively, subsection (1) is amended, a new subsection (5) is added to that section, and subsection (2) is republished, to read:

815.06 Offenses against users of computers, computer systems, computer networks, and electronic devices.—

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

(a)1. "Ransomware" means a computer contaminant or lock placed or introduced without authorization into a computer, computer system, computer network, or electronic device which does any of the following:

a. Restricts access by an authorized person to the computer, computer system, computer network, or electronic device or to any data held by the computer, computer system, computer network, or electronic device under circumstances in which the person responsible for the placement or introduction of the computer contaminant or lock demands payment of money or other consideration to:

(I) Remove the computer contaminant or lock;

(II) Restore access to the computer, computer system, computer network, electronic device, or data; or

(III) Otherwise remediate the impact of the computer contaminant or lock; or

b. Transforms data held by the computer, computer system, or computer network, or electronic device into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key.

2. The term does not include authentication required to upgrade or access purchased content or the blocking of access to subscription content in the case of nonpayment for the access.

(b) "User" means a person with the authority to operate or maintain a computer, computer system, computer network, or electronic device.

(2) A person commits an offense against users of computers, computer systems, computer networks, or electronic devices if he or she willfully, knowingly, and without authorization or exceeding authorization:

(a) Accesses or causes to be accessed any computer, computer system, computer network, or electronic device with knowledge that such access is unauthorized or the manner of use exceeds authorization;

(b) Disrupts or denies or causes the denial of the ability to transmit data to or from an authorized user of a computer, computer system, computer network, or electronic device, which, in whole or in part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another;

(c) Destroys, takes, injures, or damages equipment or supplies used or intended to be used in a computer, computer system, computer network, or electronic device;

(d) Destroys, injures, or damages any computer, computer

system, computer network, or electronic device;

(e) Introduces any computer contaminant into any computer, computer system, computer network, or electronic device; or

(f) Engages in audio or video surveillance of an individual by accessing any inherent feature or component of a computer, computer system, computer network, or electronic device, including accessing the data or information of a computer, computer system, computer network, or electronic device that is stored by a third party.

(5)(a)1. A person who places ransomware in a computer, computer system, computer network, or electronic device commits a felony of the first degree, punishable as provided in s. 775.082 or s. 775.084, and shall be assessed a fine equal to or twice the amount of ransom demanded in the attack or the maximum fine provided under s. 775.083, whichever is greater.

2. Notwithstanding any other law, fines collected under this subsection must be distributed as follows:

a. Half of the fine must be provided to the Florida Digital Service to be used for cybersecurity operations.

b. Half of the fine must be divided equally among law enforcement agencies and private entities or individuals who aided in the apprehension and conviction of the defendant.

(b) An employee or a contractor of the government of this state or a local government, as defined in s. 215.89(2)(c), who knowingly and intentionally provides access to a person who commits a violation of:

1. Subsection (2); or

2. This subsection,

commits a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

Section 4. For the 2022-2023 fiscal year, the sum of $1 million in nonrecurring funds is appropriated to the Florida Digital Service, which shall disburse the funds to local governments for the training required under s. 282.3185(3), Florida Statutes.

Section 5. This act shall take effect July 1, 2022.