A bill to be entitled

An act relating to public records; amending s. 119.0713, F.S.; providing an exemption from public records requirements for certain information held by a utility owned or operated by a unit of local government; providing definitions; providing retroactive application; providing for future legislative review and repeal of the exemption; providing a statement of public necessity; providing an effective date.

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

Section 1. Subsection (5) of section 119.0713, Florida Statutes, is amended to read:

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

(5)(a) The following information held by a utility owned or operated by a unit of local government is exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution:

1. Information related to the security of the technology, processes, or practices of a utility owned or operated by a unit of local government that are designed to protect the utility's networks, computers, programs, and data from attack, damage, or unauthorized access, which information, if disclosed, would

facilitate the alteration, disclosure, or destruction of such data or information technology resources.

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

3. Information related to threat detection, defense, deterrence, or response plans and actions for information technology and operational technology systems of a utility owned or operated by a unit of local government, including, but not limited to, plans and actions made or taken in response to a ransomware attack or cyberattack on or threat to information technology or operational technology systems.

4. Information related to insurance or other risk mitigation products or coverages, including, but not limited to, deductible or self-insurance amounts, coverage limits, and policy terms and conditions, for the protection of the information technology and operational technology systems and data of a utility owned or operated by a unit of local government.

5. Critical energy infrastructure information created or received by a utility owned or operated by a unit of local

government. As used in this subparagraph, the term:

a. "Critical energy infrastructure information" means specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure which:

(I) Includes details about the production, generation, transportation, transmission, or distribution of energy;

(II) Could be useful in planning an attack on critical infrastructure; and

(III) Provides more detailed location information than the general location of the critical infrastructure.

b. "Critical infrastructure" means existing and proposed systems and assets, whether physical or virtual, the incapacity or destruction of which would negatively affect security, economic security, public health, or public safety.

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

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

(c) This subsection is subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2027 ~~2024~~, unless reviewed and saved from repeal through reenactment by the Legislature.

Section 2. The Legislature finds that it is a public

necessity that information held by a utility owned or operated by a unit of local government and relating to the utility's threat detection, defense, or deterrence of increasing ransomware attacks or cyberattacks from foreign or domestic terrorists; information regarding the insurance coverage amounts, premium amount paid, self-insurance amounts, and policy terms and conditions of such cybersecurity insurance policies held by a utility owned or operated by a unit of local government; and critical energy infrastructure information created or received by the utility which consists of details about the production, generation, transportation, transmission, or distribution of energy be made exempt from s. 119.07(1), Florida Statutes, and s. 24(a), Article I of the State Constitution. Such information held by a utility owned or operated by a local government is critical information, the release of which could lead to extreme danger or harm to the citizens of this state. Typical critical energy infrastructure information held by a utility consists of critical asset location, vulnerable electric grid transmission information, emerging technologies utilized by the utility to prevent a cyberattack, and secure information that utilities in the state share with regional and federal entities. The exposure or leak of such information could lead to interruptions in the delivery of essential services, as well as financial or physical harm to the citizens of the state. Critical energy infrastructure

information has been defined and codified in law in over half of the states in the United States of America in conjunction with the Federal Energy Regulatory Commission. Utilities in the state have recently been attacked by criminals who hold hostage critical data and operability of the utility for ransom. Public disclosure of insurance coverages provides information to potential attackers as to the monetary limits to which they may seek ransom from these utilities. These vulnerabilities leave all utilities owned and operated by a unit of local government, which control water, electricity, wastewater, and natural gas utilities throughout this state, exposed to cyberattacks and ransom demands. The Legislature finds that the harm that may result from the release of such information outweighs any public benefit that may be derived from disclosure of the information.

Section 3. This act shall take effect July 1, 2022.