CHAPTER 2023-32

Committee Substitute for
Committee Substitute for Senate Bill No. 258

An act relating to prohibited applications on government-issued devices; creating s. 112.22, F.S.; defining terms; requiring public employers to take certain actions relating to prohibited applications; prohibiting employees and officers of public employers from downloading or accessing prohibited applications on government-issued devices; providing exceptions; providing a deadline by which specified employees must remove, delete, or uninstall a prohibited application; requiring the Department of Management Services to compile a specified list and establish procedures for a specified waiver; authorizing the department to adopt emergency rules; requiring that such rulemaking occur within a specified timeframe; requiring the department to adopt specified rules; providing a declaration of important state interest; providing an effective date.

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

Section 1. Section 112.22, Florida Statutes, is created to read:

112.22 Use of applications from foreign countries of concern prohibited.

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

(a) "Department" means the Department of Management Services.

(b) "Employee or officer" means a person who performs labor or services for a public employer in exchange for salary, wages, or other remuneration.

(c) "Foreign country of concern" means the People's Republic of China, the Russian Federation, the Islamic Republic of Iran, the Democratic People's Republic of Korea, the Republic of Cuba, the Venezuelan regime of Nicolás Maduro, or the Syrian Arab Republic, including any agency of or any other entity under significant control of such foreign country of concern.

(d) "Foreign principal" means:

1. The government or an official of the government of a foreign country of concern;

2. A political party or a member of a political party or any subdivision of a political party in a foreign country of concern;

3. A partnership, an association, a corporation, an organization, or another combination of persons organized under the laws of or having its principal place of business in a foreign country of concern, or an affiliate or a subsidiary thereof; or

4. Any person who is domiciled in a foreign country of concern and is not a citizen or a lawful permanent resident of the United States.

(e) "Government-issued device" means a cellular telephone, desktop computer, laptop computer, computer tablet, or other electronic device capable of connecting to the Internet which is owned or leased by a public employer and issued to an employee or officer for work-related purposes.

(f) "Prohibited application" means an application that meets the following criteria:

1. Any Internet application that is created, maintained, or owned by a foreign principal and that participates in activities that include, but are not limited to:

a. Collecting keystrokes or sensitive personal, financial, proprietary, or other business data;

b. Compromising e-mail and acting as a vector for ransomware deployment;

c. Conducting cyber-espionage against a public employer;

d. Conducting surveillance and tracking of individual users; or

e. Using algorithmic modifications to conduct disinformation or misinformation campaigns; or

2. Any Internet application the department deems to present a security risk in the form of unauthorized access to or temporary unavailability of the public employer's records, digital assets, systems, networks, servers, or information.

(g) "Public employer" means the state or any agency, authority, branch, bureau, commission, department, division, special district, institution, university, institution of higher education, or board thereof; or any county, district school board, charter school governing board, or municipality, or any agency, branch, department, board, or metropolitan planning organization thereof.

(2)(a) A public employer shall do all of the following:

1. Block all prohibited applications from public access on any network and virtual private network that it owns, operates, or maintains.

2. Restrict access to any prohibited application on a government-issued device.

3. Retain the ability to remotely wipe and uninstall any prohibited application from a government-issued device that is believed to have been adversely impacted, either intentionally or unintentionally, by a prohibited application.

(b) A person, including an employee or officer of a public employer, may not download or access any prohibited application on any government-issued device.

1. This paragraph does not apply to a law enforcement officer as defined in s. 943.10(1) if the use of the prohibited application is necessary to protect the public safety or conduct an investigation within the scope of his or her employment.

2. A public employer may request a waiver from the department to allow designated employees or officers to download or access a prohibited application on a government-issued device.

(c) Within 15 calendar days after the department issues or updates its list of prohibited applications pursuant to paragraph (3)(a), an employee or officer of a public employer who uses a government-issued device must remove, delete, or uninstall any prohibited applications from his or her government-issued device.

(3) The department shall do all of the following:

(a) Compile and maintain a list of prohibited applications and publish the list on its website. The department shall update this list quarterly and shall provide notice of any update to public employers.

(b) Establish procedures for granting or denying requests for waivers pursuant to subparagraph (2)(b)2. The request for a waiver must include all of the following:

1. A description of the activity to be conducted and the state interest furthered by the activity.

2. The maximum number of government-issued devices and employees or officers to which the waiver will apply.

3. The length of time necessary for the waiver. Any waiver granted pursuant to subparagraph (2)(b)2. must be limited to a timeframe of no more than 1 year, but the department may approve an extension.

4. Risk mitigation actions that will be taken to prevent access to sensitive data, including methods to ensure that the activity does not connect to a state system, network, or server.

5. A description of the circumstances under which the waiver applies.

(4)(a) Notwithstanding s. 120.74(4) and (5), the department is authorized, and all conditions are deemed met, to adopt emergency rules pursuant to s. 120.54(4) and to implement paragraph (3)(a). Such rulemaking must occur initially by filing emergency rules within 30 days after July 1, 2023.

(b) The department shall adopt rules necessary to administer this section.

Section 2. The Legislature finds that a proper and legitimate state purpose is served when efforts are taken to secure a public employer's system, network, or server. Therefore, the Legislature determines and declares that this act fulfills an important state interest.

Section 3. This act shall take effect July 1, 2023.

Approved by the Governor May 8, 2023.

Filed in Office Secretary of State May 8, 2023.