

1 A bill to be entitled

2 An act relating to prohibited applications on
 3 government-issued devices; creating s. 112.22, F.S.;
 4 defining terms; requiring public employers to take
 5 certain actions relating to prohibited applications;
 6 prohibiting persons, including employees and officers
 7 of public employers, from downloading or accessing
 8 prohibited applications on government-issued devices;
 9 providing exceptions; providing a deadline by which
 10 specified employees and officers must remove, delete,
 11 or uninstall a prohibited application; requiring the
 12 Department of Management Services to compile and
 13 maintain a specified list and establish procedures for
 14 a specified waiver; authorizing the department to
 15 adopt emergency rules; requiring that such rulemaking
 16 occur within a specified timeframe; requiring the
 17 department to adopt rules; providing a declaration of
 18 important state interest; providing an effective date.
 19

20 Be It Enacted by the Legislature of the State of Florida:
 21

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

24 112.22 Use of applications from foreign countries of
 25 concern prohibited.—

- 26 (1) As used in this section, the term:
- 27 (a) "Department" means the Department of Management
 28 Services.
- 29 (b) "Employee or officer" means a person who performs
 30 labor or services for a public employer in exchange for salary,
 31 wages, or other remuneration.
- 32 (c) "Foreign country of concern" means the People's
 33 Republic of China, the Russian Federation, the Islamic Republic
 34 of Iran, the Democratic People's Republic of Korea, the Republic
 35 of Cuba, the Venezuelan regime of Nicolás Maduro, or the Syrian
 36 Arab Republic, including any agency of or any other entity under
 37 significant control of such foreign country of concern.
- 38 (d) "Foreign principal" means:
- 39 1. The government or an official of the government of a
 40 foreign country of concern;
- 41 2. A political party or a member of a political party or
 42 any subdivision of a political party in a foreign country of
 43 concern;
- 44 3. A partnership, an association, a corporation, an
 45 organization, or another combination of persons organized under
 46 the laws of or having its principal place of business in a
 47 foreign country of concern, or an affiliate or a subsidiary
 48 thereof; or
- 49 4. Any person who is domiciled in a foreign country of
 50 concern and is not a citizen or lawful permanent resident of the

51 United States.

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

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

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

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

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

66 c. Conducting cyber-espionage against a public employer;

67 d. Conducting surveillance and tracking of individual
68 users; or

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

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

75 (g) "Public employer" means the state or any agency,

76 authority, branch, bureau, commission, department, division,
77 special district, institution, university, institution of higher
78 education, or board thereof; or any county, district school
79 board, charter school governing board, or municipality, or any
80 agency, branch, department, board, or metropolitan planning
81 organization thereof.

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

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

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

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

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

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

99 2. A public employer may request a waiver from the
100 department to allow designated employees or officers to download

101 or access a prohibited application on a government-issued
102 device.

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

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

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

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

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

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

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

125 4. Risk mitigation actions that will be taken to prevent

126 access to sensitive data, including methods to ensure that the
127 activity does not connect to a state system, network, or server.

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

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

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

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

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