

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 of the United States.

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

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

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

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

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

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

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

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

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

74 (g) "Public employer" means the state or any agency,
75 authority, branch, bureau, commission, department, division,

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

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

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

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

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

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

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

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

101 device.

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

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

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

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

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

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

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

124 4. Risk mitigation actions that will be taken to prevent
125 access to sensitive data, including methods to ensure that the

126 activity does not connect to a state system, network, or server.

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

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

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

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

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