HOUSE BILL NO. 5065

September 28, 2023, Introduced by Reps. Fink, Thompson, Hoadley, Alexander, Bierlein, Meerman, DeBoyer, Maddock, Bruck, Johnsen, Smit, Jaime Greene, Markkanen, Cavitt, Rigas, Kunse and Schmaltz and referred to the Committee on Government Operations.

A bill to prohibit the use of certain applications on government-issued devices; to require public employers to take certain actions related to prohibited applications; to prohibit certain employees or officers from downloading or accessing certain applications; to provide exceptions; and to provide for the powers and duties of certain state and local governmental officers and entities.

THE PEOPLE OF THE STATE OF MICHIGAN ENACT:

Sec. 1. This act may be cited as the "prohibited applications on government-issued devices act".

Sec. 3. The legislature finds that a proper and legitimate state purpose is served when efforts are taken to secure the system, network, or server of a public employer. Therefore, the legislature determines and declares that this act fulfills an important state interest.

Sec. 5. As used in this act:

(a) "Department" means the department of technology, management, and budget.

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

(c) "Foreign country of concern" means any of the following:

(*i*) The People's Republic of China.

(*ii*) The Russian Federation.

(*iii*) The Islamic Republic of Iran.

(*iv*) The Democratic People's Republic of Korea.

(*v*) The Republic of Cuba.

(*vi*) The Venezuelan regime of Nicolás Maduro.

(*vii*) The Syrian Arab Republic.

(*viii*) Any agency of or any other entity under significant control of an entity listed under subdivisions (*i*) to (*vii*).

(d) "Foreign principal" means any of the following:

(*i*) The government or an official of the government of a foreign country of concern.

(*ii*) A political party, a member of a political party, or any subdivision of a political party in a foreign country of concern.

(*iii*) A partnership, an association, a corporation, an organization, or a 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 of a partnership, an association, a corporation, an organization, or a combination of persons organized under the laws of or having its principal place of business in a foreign country of concern.

(*iv*) Any individual 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, a desktop computer, a laptop computer, or other electronic device that is capable of connecting to the internet owned or leased by a public employer and issued to an employee or officer for work-related purposes.

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

(*i*) Is created, maintained, or owned by a foreign principal and participates in activities that include, but are not limited to, any of the following:

(A) Collects keystrokes or sensitive personal, financial, proprietary, or other business data.

(B) Compromises emails and acts as a vector for ransomware deployment.

(C) Conducts cyber-espionage against a public employer.

(D) Conducts surveillance and tracks individual users.

(E) Uses algorithmic modifications to conduct disinformation or misinformation campaigns.

(*ii*) The department considers 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 this state; a local unit of government or other political subdivision of this state; any intergovernmental, metropolitan, or local department, agency, or authority, or other local political subdivision; a school district, a public school academy, or an intermediate school district, as those terms are defined in sections 4 to 6 of the revised school code, 1976 PA 451, MCL 380.4 to 380.6; a community college or junior college described in section 7 of article VIII of the state constitution of 1963; or an institution of higher education described in section 4 of article VIII of the state constitution of 1963.

Sec. 7. (1) Except as otherwise provided in subsection (3), a public employer shall do all of the following:

(a) Block a prohibited application from public access on any network and virtual private network owned, operated, or maintained by that public employer.

(b) Restrict access to any prohibited application on a government-issued device.

(c) 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.

(2) A person, including an employee or officer, may not download or access a prohibited application on any government-issued device. This subsection does not apply to a law enforcement officer if the use of the prohibited application is necessary to protect the public safety or conduct of an investigation within the scope of the law enforcement officer's employment.

(3) A public employer may request a waiver from the department to allow a designated employee or officer to download or access a prohibited application on a government-issued device. A request for a waiver pursuant to this subsection must be in writing and include all of the following:

(a) A description of the activity to be conducted and the state interest furthered by the activity.

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

(c) The length of time necessary for the waiver. A waiver granted pursuant to this subsection must be limited to a time frame of no more than 1 year, but the department may approve an extension.

(d) 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.

(e) A description of the circumstances under which the waiver applies.

Sec. 9. (1) Within 90 days after the effective date of this act, the department shall do both of the following:

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

(b) Establish procedures for granting or denying a waiver.

(2) Within 15 calendar days after the department issues or updates the list of prohibited applications pursuant to subsection (1)(a), an employee or officer who uses a government-issued device

must remove, delete, or uninstall any prohibited application from the employee's or officer's government-issued device.

Sec. 11. The department shall adopt rules necessary to administer this section.

Enacting section 1. This act takes effect July 1, 2023.