

PROHIBITED APPLICATIONS ON GOVERNMENT-ISSUED DEVICES

Phone: (517) 373-8080
<http://www.house.mi.gov/hfa>

House Bill 4235 as introduced
Sponsor: Rep. Rachelle Smit
Committee: Government Operations
Complete to 3-19-25

Analysis available at
<http://www.legislature.mi.gov>

SUMMARY:

House Bill 4235 would create a new act, the Prohibited Applications on Government-Issued Devices Act, to require a **public employer** to do all of the following:

- Block a **prohibited application** from public access on any network and virtual private network owned, operated, or maintained by the public employer.
- Restrict access to any prohibited application on a **government-issued device**.
- Retain the ability to remotely wipe and uninstall any prohibited application from a government-issued device that is believed to have been adversely affected, either intentionally or unintentionally, by a prohibited application.

Public employer would mean any of the following:

- The state.
- A local unit of government or other political subdivision of the state.
- Any intergovernmental, metropolitan, or local department, agency, or authority, or other local political subdivision.
- A school district, public school academy, or intermediate school district.
- A public community college or junior college.
- A state university.

Prohibited application would mean an internet application that meets the following criteria:

- It is created, maintained, or owned by a **foreign principal** and participates in activities that include any of the following:
 - Collecting keystrokes or sensitive personal, financial, proprietary, or business data.
 - Compromising emails and acts as a vector for ransomware deployment.
 - Conducting cyber-espionage against a public employer.
 - Conducting surveillance and tracking individual users.
 - Using algorithmic modifications to conduct disinformation campaigns or misinformation campaigns.
- The Department of Technology, Management, and Budget (DTMB) considers it 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.

Foreign principal would mean any of the following:

- The government or a government official of a **foreign country of concern**.

- A political party in a foreign country of concern or a member or subdivision of such a political party.
- A partnership, association, corporation, organization, or combination of persons that is organized under the laws of a foreign country of concern or that has its principal place of business in a foreign country of concern or an affiliate or subsidiary of such an entity.
- An individual who is domiciled in a foreign country of concern and is not a citizen or lawful permanent resident of the United States.

Foreign country of concern would mean China, Cuba, Iran, North Korea, Russia, Syria, or Venezuela or an agency or other entity under significant control of any of those countries.

Government-issued device would mean a cellphone, a desktop or laptop computer, or another electronic device capable of connecting to the internet that is owned or leased by a public employer and issued for work-related purposes to an employee or officer (an individual who performs labor or services for a public employer for salary, wages, or other remuneration).

Prohibition and waiver

The bill also would prohibit a person, including an employee or officer, from downloading or accessing a prohibited application on a government-issued device. This provision would not apply to a law enforcement officer if the use of the prohibited application is necessary to protect the public safety or to conduct an investigation within the scope of their employment.

A public employer could request a waiver from DTMB to allow a designated employee or officer to download or access a prohibited application on a government-issued device. The request would have to be in writing and include all of the following:

- A description of the activity to be conducted and the state interest furthered by the activity.
- The maximum number of government-issued devices and employees or officers the waiver will apply to.
- The length of time necessary for the waiver. A waiver's time frame could not exceed one year, but DTMB could approve an extension.
- 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.
- A description of the circumstances the waiver applies under.

DTMB would have to establish procedures for granting or denying a waiver within 90 days after the bill takes effect.

List of prohibited applications

Within 90 days after the bill takes effect, DTMB would have to compile, and publish on its website, a list of all prohibited applications. DTMB would have to update the list quarterly and provide notice of updates to all public employers. No later than 15 calendar days after the list is issued or updated, an employee or officer who uses a government-issued device would have to remove, delete, or uninstall an application on the list from their government-issued device.

Other provisions

DTMB would have to develop and issue rules to implement the bill.

The bill would take effect July 1, 2025.

FISCAL IMPACT:

Implementation of HB 4235 would require some additional administrative resources and staff time for public employers, including the state, local units of government, schools, community colleges and universities. However, the bill is not expected to result in more than nominal costs. The Department of Technology, Management, and Budget may incur some additional costs related to administrative responsibilities required of it in the bill.

Public employers would be required to have the technical ability to block, restrict, and remotely wipe and uninstall prohibited applications. A public employer who does not already have this ability would incur marginal costs of acquiring software subscription plans, which are less than \$100 per year.

DTMB would be responsible for promulgating rules to implement the bill, compiling and maintaining a list of prohibited applications, and granting or denying requests for waivers from the prohibition. It is not yet known if DTMB would be able to absorb these responsibilities with existing staff. The average cost of a state FTE position is approximately \$128,000 per year.

Legislative Analyst: Rick Yuille
Fiscal Analyst: Michael Cnossen

■ This analysis was prepared by nonpartisan House Fiscal Agency staff for use by House members in their deliberations and does not constitute an official statement of legislative intent.