Senate

General Assembly

File No. 566

January Session, 2023

Substitute Senate Bill No. 1191

Senate, April 13, 2023

The Committee on Government Administration and Elections reported through SEN. FLEXER of the 29th Dist., Chairperson of the Committee on the part of the Senate, that the substitute bill ought to pass.

AN ACT PROHIBITING THE USE OF A CERTAIN APPLICATION, SOFTWARE AND PROGRAMS ON STATE GOVERNMENT DEVICES AND REQUIRING MINIMUM SECURITY STANDARDS AND ANNUAL AUDITS OF SUCH DEVICES.

Be it enacted by the Senate and House of Representatives in General Assembly convened:

Section 1. (NEW) (*Effective July 1, 2023*) (a) As used in this section and section 2 of this act:

(1) "Public official" means any state-wide elected officer, member or member-elect of the General Assembly, person appointed to any office of the legislative, judicial or executive branch of state government by the Governor or an appointee of the Governor, with or without the advice and consent of the General Assembly, person appointed or elected by the General Assembly or by any member of either house thereof and judge of any court either elected or appointed, but does not include a member of an advisory board or a senator or representative in Congress;

(2) "State employee" means any full or part-time employee in the

executive, legislative or judicial branch of state government, whether in the classified or unclassified service; and

(3) "State-issued device" means any electronic equipment capable of connecting to the Internet that is owned or leased by the state, including, but not limited to, any cellular phone, computer, laptop, tablet or any other similar technology.

(b) On and after October 1, 2023, no public official or state employee shall use any state-issued device to access, upload content to or download the Internet web site or the application TikTok, except a public official or state employee may access TikTok for law enforcement purposes.

(c) On and after December 1, 2023, no public official or state employee shall use any computer program, software, application or state-issued device that has been prohibited under the security standards developed pursuant to subsections (b) and (c) of section 2 of this act.

Sec. 2. (NEW) (*Effective July 1, 2023*) (a) As used in this section, "cybersecurity threat" means any activity intended to result in unauthorized access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality or availability of the state's information technology system or information stored on, or transiting, the state's information technology system.

(b) Not later than September 1, 2023, and not less than quarterly thereafter, the Chief Information Officer and Chief Information Security Officer within the Department of Administrative Services, director of the Office of Information Technology Services and Chief Court Administrator, or their designees, shall communicate regarding any known or potential cybersecurity threats to the state's information technology systems and state-issued devices, and not later than December 1, 2023, shall jointly develop minimum security standards that apply to all three branches of state government regarding computer programs, software, applications and state-issued devices used by public officials and state employees to counter cybersecurity threats,

with any modifications for an individual branch deemed necessary by said officers, said director and the Chief Court Administrator. Such standards shall be revised periodically, as often as deemed necessary by said officers, director and the Chief Court Administration, provided such standards shall be revised not less than annually. Notwithstanding the provisions of section 4-166 of the general statutes, such standards shall not be deemed a regulation for purposes of chapter 54 of the general statutes.

(c) As part of the standards developed under subsection (b) of this section, said officers, said director and the Chief Court Administrator may jointly prohibit the use within state government of any computer program, software, application or brand of state-issued device that they deem to violate such standards or otherwise pose a cybersecurity threat. Any such prohibition shall be posted on the Internet websites of all three branches of government and shall be communicated electronically to all state employees and public officials.

(d) Not later than July 1, 2024, and annually thereafter, the Chief Information Officer within the Department of Administrative Services or a designee shall conduct an audit of the state-issued devices and computer programs, software and applications used on such devices by public officials and state employees within the executive branch to ensure that such devices, programs, software and applications comply with the minimum security standards established under this section.

(e) In the case of state-issued devices used by public officials and state employees within the legislative branch, not later than July 1, 2024, and annually thereafter, the director of the Office of Information Technology Services or a designee shall conduct such audit to comply with the minimum security standards established under this section.

(f) In the case of state-issued devices used by public officials and state employees within the judicial branch, not later than July 1, 2024, and annually thereafter, the Chief Court Administrator or a designee shall conduct such audit to comply with the minimum security standards established under this section.

This act shall take effect as follows and shall amend the following sections:		
Section 1	*July 1, 2023*	New section
Sec. 2	*July 1, 2023*	New section

Statement of Legislative Commissioners:
Section 2(b) was reorganized into subsections (b) and (c) for consistency with standard drafting conventions.

GAE *Joint Favorable Subst. -LCO*

The following Fiscal Impact Statement and Bill Analysis are prepared for the benefit of the members of the General Assembly, solely for purposes of information, summarization and explanation and do not represent the intent of the General Assembly or either chamber thereof for any purpose. In general, fiscal impacts are based upon a variety of informational sources, including the analyst's professional knowledge. Whenever applicable, agency data is consulted as part of the analysis, however final products do not necessarily reflect an assessment from any specific department.

OFA Fiscal Note

State Impact: None

Municipal Impact: None

Explanation

This bill has no fiscal impact. The purpose of the bill is to ban certain applications including Tiktok from state devices. This does not obligate the state to any further action.

The Out Years

State Impact: None

Municipal Impact: None

OLR Bill Analysis

SB 1191

AN ACT PROHIBITING THE USE OF A CERTAIN APPLICATION, SOFTWARE AND PROGRAMS ON STATE GOVERNMENT DEVICES AND REQUIRING MINIMUM SECURITY STANDARDS AND ANNUAL AUDITS OF SUCH DEVICES.

SUMMARY

Starting October 1, 2023, this bill prohibits state employees and public officials from using any state-issued device to access, upload content to, or download the TikTok website or application, except for law enforcement purposes. The bill's prohibition applies to (1) full- and part-time employees in all three branches of state government, whether in the classified or unclassified service ("state employees") and (2) the following "public officials": (1) statewide elected officers, (2) legislators and legislators-elect, (3) judges, (4) gubernatorial appointees, and (5) people appointed or elected by the General Assembly or either chamber. It does not apply to advisory board members and members of Congress.

The bill designates four state officials to:

1. periodically communicate known or potential cybersecurity threats to state systems and devices;

2. develop and periodically revise minimum security standards for state government; and

3. annually audit all state-issued devices and computer programs, software, and applications used on them to ensure they comply with the standards.

Starting December 1, 2023, it bars state employees and public officials from using any computer program, software, application, or state-

issued device that these minimum security standards prohibit.

EFFECTIVE DATE: July 1, 2023

MINIMUM SECURITY STANDARDS FOR STATE SYSTEMS AND DEVICES

Communication of Cybersecurity Threats

Starting by September 1, 2023, and at least quarterly afterwards, the Department of Administrative Services' (DAS) chief information officer and chief information security officer, Office of Information Technology Services director, and chief court administrator, or their designees, must communicate any known or potential cybersecurity threats to the state's information technology systems and state-issued devices.

Under the bill, a "cybersecurity threat" is any activity intended to result in unauthorized access or impairment to, or exfiltration or manipulation of, the integrity, confidentiality, or availability of the state's information technology system or information stored on, or moving through, the system. A "state-issued device" is any state-owned or -leased electronic equipment that can connect to the Internet, including cellphones, computers, laptops, tablets, and other similar technology.

Development of Minimum Security Standards

By December 1, 2023, the bill requires these officials to jointly develop minimum security standards for all three branches of state government on computer programs, software, applications, and state-issued devices used by public officials and state employees to counter cybersecurity threats. These standards may include any modifications for an individual branch they find necessary. They must periodically revise the standards, as often as they find necessary, but at least annually. The standards are not deemed a regulation.

Prohibited Programs and Devices

Under the bill, the standards may prohibit the use of any computer program, software, application, or brand of state-issued device that the officials find violates the standards or otherwise poses a cybersecurity

threat. This prohibition must be posted on each branch's website and communicated electronically to all state employees and public officials.

Required Audits in Each Branch of State Government

Annually, starting by July 1, 2024, the bill requires audits of state-issued devices and the computer programs, software, and applications used on them to ensure they comply with the minimum security standards. The DAS chief information officer, Office of Information Technology Services director, and chief court administrator, or their designees, must do these audits for public officials and state employees in the executive, legislative, and judicial branches, respectively.

COMMITTEE ACTION

Government Administration and Elections Committee

Joint Favorable
Yea 18 Nay 1 (03/24/2023)