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)