The Florida Senate

BILL ANALYSIS AND FISCAL IMPACT STATEMENT

(This document is based on the provisions contained in the legislation as of the latest date listed below.)

Prepared By: The Professional Staff of the Committee on Fiscal Policy

BILL:	CS/SB 258
INTRODUCER:	Governmental Oversight and Accountability Committee and Senator Burgess
SUBJECT:	Prohibited Applications on Government-issued Devices
DATE:	March 22, 2023 REVISED:

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Harmsen	McVaney	GO	**Fav/CS**
2.	Harmsen	Yeatman	FP	**Pre-Meeting**

Please see Section IX. for Additional Information:

COMMITTEE SUBSTITUTE - Substantial Changes

I. Summary:

CS/SB 258 instructs the Department of Management Services (DMS) to create a list of prohibited applications, defined as those that (1) are created, maintained, or owned by a foreign principal and that engage in specific activities that endanger cybersecurity; or (2) present a security risk in the form of unauthorized access to or temporary unavailability of a public employer's information technology systems or data, as determined by the DMS. This definition will likely include TikTok and WeChat.

The bill requires public employers (including state agencies, public education institutions, and local governments) to:

- Block access to prohibited applications on any wireless network or virtual private network that it owns, operates, or maintains;
- Restrict access to prohibited applications on any government-issued device; and
- Retain the ability to remotely wipe and uninstall prohibited applications from a compromised government-issued device.

All persons are prohibited from downloading prohibited applications on a government-issued device, and officers and employees of a public employer must remove any prohibited application from their government-issued device within 15 calendar days of the DMS' issuance of a list of prohibited applications.

The bill allows the use of prohibited applications by law enforcement officers, if the use is necessary to protect the public safety or to conduct an investigation. It also allows other government employees to use a prohibited application, if they are granted a waiver by the DMS.

The bill provides emergency rulemaking authority to the DMS to adopt a list of prohibited applications, and general rulemaking authority to implement a process by which it can grant waivers from the prohibition.

The impact on state and local government expenditures is indeterminate.

The bill takes effect on July 1, 2023.

II. Present Situation:

TikTok and WeChat

TikTok is a smartphone application that allows its more than 1 billion global users, of which 113 million are U.S.-based, to share videos with each other.[1] TikTok is owned by ByteDance Ltd., a privately held company incorporated in the Cayman Islands, with a headquarters in Beijing, China.[2] WeChat is a smartphone application that offers multiple functions, including messaging, payment processing, ridesharing, and photo sharing with an estimated 1 billion monthly active users.[3] WeChat is owned by TenCent Holdings, Ltd., a publicly traded corporation that is headquartered in China.[4] Both applications, by permissions of their users, collect several data points from their users, including location data and internet address, and the type of device that is used to access the application. The applications share the ability to collect GPS data, network contacts, and user information (e.g., age and preferred content).[5]

These companies are under increasing scrutiny by the U.S. government as a potential privacy and security risk to U.S. citizens.[6] This is because they, like all technology companies that do business in China, are subject to Chinese laws that require companies that operate in the country to turn over user data, intellectual property, and proprietary commercial secrets when requested

---

[1] DATAREPORTAL.COM, *TikTok Statistics and Trends* (Jan. 2023), https://datareportal.com/essential-tiktok-stats (last visited Mar. 14, 2023).
[2] ByteDance, Inc., *About Us*, https://www.bytedance.com/en/ (last visited Mar. 14, 2023). *See also*, NEWSWEEK, Chloe Mayer, *Is TikTok Owned by the Chinese Communist Party?* (Oct. 17, 2022), *available at* https://www.newsweek.com/tiktok-owned-controlled-china-communist-party-ccp-influence-1752415 (last visited Mar. 14, 2023).
[3] CONGRESSIONAL RESEARCH SERVICE, Patricia Moloney Figliola, *TikTok: Technology Overview and Issues* (Dec. 4, 2020), https://crsreports.congress.gov/product/pdf/R/R46543 (last visited Mar. 14, 2023).
[4] BUSINESS OF APPS, Mansoor Iqbal, *WeChat Revenue and Usage Statistics* (2022) (Sept. 6, 2022) https://www.businessofapps.com/data/wechat-statistics/ (last visited Mar. 14, 2023).
[5] WeChat, *WeChat Privacy Policy* (Sept. 9, 2022), https://www.wechat.com/en/privacy_policy.html (last visited Mar. 14, 2023).
6 *See, e.g.*, Federal Bureau of Investigation, Remarks delivered by Director Christopher Wray, *The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States* (Jul. 7, 2020), *available at* https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states (last visited Mar. 14, 2023).

by the government.[7] TikTok recently moved its U.S. data servers to U.S. locations to "help to protect against unauthorized access to user data."[8] In one instance, confirmed by TikTok, two employees improperly used the application's data to track the location of journalists who wrote a negative story about the business; one employee was fired and another resigned as a result of their improper actions.[9]

There are also allegations that TikTok manipulates its algorithm to provide misinformation to its users.[10]

Federal, State, and Local Actions

In August 2020, President Trump signed two executive orders that prohibited commercial transactions between U.S. citizens and TikTok [11] and required ByteDance to divest from any asset that supports TikTok's U.S.-arm.[12] President Trump also took similar action proposing to ban transactions with WeChat.[13] While these executive orders were subject to injunction in different courts, they were revoked ultimately by a subsequent executive order issued by President Biden.

Congress passed the "No TikTok on Government Devices Act" as part of the omnibus spending bill in December 2022.[14] The law directs the Office of Management and Budget (OMB) to create standards and guidelines for the removal of TikTok from government devices. On February 27, 2023, the OMB issued guidance that requires all executive agencies and their contractors that use IT[15] to remove and disallow installations of TikTok within 30 days.[16] The guidance allows

---

[7] Nazak Nikakhtar, U.S. *Businesses Must Navigate Significant Risk of Chinese Government Access to Their Data* (Mar. 22, 2021), https://www.jdsupra.com/legalnews/u-s-businesses-must-navigate-3014130/ (last visited Mar. 14, 2023). *See also*, note 3, *supra* at p. 6.
[8] TikTok, *Delivering on our US Data Governance* (Jun. 17, 2022), https://newsroom.tiktok.com/en-us/delivering-on-our-us-data-governance (last visited Mar. 14, 2023).
[9] FORBES, Emily Baker-White, *Exclusive: TikTok Spied on Forbes Journalists* (Dec. 22, 2022), https://www.forbes.com/sites/emilybaker-white/2022/12/22/tiktok-tracks-forbes-journalists-bytedance/?sh=3bd5d3327da5 (last visited Mar. 14, 2023).
[10] AP NEWS, Haleluya Hadero, *Why TikTok is Being Banned on Government Phones in US and Beyond* (Feb. 28, 2023) https://apnews.com/article/why-is-tiktok-being-banned-7d2de01d3ac5ab2b8ec2239dc7f2b20d (last visited Mar. 14, 2023).
[11] President Donald J. Trump, *Executive Order on Addressing the Threat Posed by TikTok* (Aug. 6, 2020), https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/ (last visited Mar. 14, 2023).
[12] President Donald J. Trump, *Executive Order Regarding the Acquisition of Musical.ly by ByteDance Ltd.* (Aug. 14, 2020), https://home.treasury.gov/system/files/136/EO-on-TikTok-8-14-20.pdf. (last visited Mar. 14, 2023).
[13] President Donald J. Trump, *Executive Order on Addressing the Threat Posed by WeChat* (Aug. 6, 2020), https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-posed-wechat/ (last visited Mar. 14, 2023).
[14] Pub. L. No. 117-328, div. R, §§101-102.
[15] "Information technology" means "any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used […] directly or is used by a contractor under a contract with the executive agency […]" and includes computers, peripheral equipment, software, firmware, services, and related resources. 40 U.S.C. §11101(6).
[16] Office of Management and Budget, *Memorandum: No TikTok on Government Devices Implementation Guidance* (Feb. 27, 2023), https://www.whitehouse.gov/wp-content/uploads/2023/02/M-23-13-No-TikTok-on-Government-Devices-Implementation-Guidance_final.pdf (last visited Mar. 14, 2023).

exceptions to the use and installation ban for the purposes of law enforcement activities, national security interests and activities, and security research.

As of March 2023, at least 24 states have enacted, through various forms of state action (but not legislation), bans on the use of high-risk software and services on state devices or over state-owned networks.[17]

On March 7, 2023, the Miami-Dade County Commission voted to ban TikTok from its county's work phones.[18]

State Information Technology Management

The Department of Management Services (DMS) oversees information technology (IT) governance and security for the executive branch of the State government.[19] The Florida Digital Service (FLDS) within the DMS was established by the Legislature in 2020;[20] the head of FLDS is appointed by the Secretary of DMS and serves as the state chief information officer (CIO).[21]

The FLDS was created to modernize state government technology and information services.[22] Accordingly, the DMS, through the FLDS, has the following powers, duties, and functions:

- Develop IT policy for the management of the state's IT resources;
- Develop an enterprise architecture;
- Establish IT project management and oversight standards for state agencies;
- Oversee state agency IT projects that cost $10 million or more and that are funded in the General Appropriations Act or any other law; and[23]
- Standardize and consolidate IT services that support interoperability, Florida's cloud first policy, and other common business functions and operations.

[17] GOVERNMENT TECHNOLOGY, Andrew Adams, *Updated; Where is TikTok Banned? Tracking State by State* (Dec. 14, 2022), https://www.govtech.com/biz/data/where-is-tiktok-banned-tracking-the-action-state-by-state (last visited Mar. 14, 2023).
[18] NBC MIAMI, Heather Walker, *Miami-Dade Commissioners Vote to Ban TikTok on County Devices* (Mar. 7, 2023), https://www.nbcmiami.com/news/local/miami-dade-commissioners-vote-to-ban-tiktok-on-county-devices/2988107/ (last visited Mar. 14, 2023).
[19] Section 282.0051, F.S.
[20] Ch. 2020-161, Laws of Fla.
[21] Section 282.0051(2)(a), F.S.
[22] Section 282.0051(1), F.S.
[23] The FLDS provides project oversight on IT projects that have a total cost of $20 million or more for the Department of Financial Services, the Department of Legal Affairs, and the Department of Agriculture and Consumer Services. Section 282.0051(1)(m), F.S.

State Cybersecurity Act

The State Cybersecurity Act[24] requires the DMS and the heads of state agencies to meet certain requirements to enhance state agencies' cybersecurity.[25] Specifically, the DMS, acting through the FLDS, must:[26]

- Assess state agency cybersecurity risks and determine appropriate security measures consistent with generally accepted best practices for cybersecurity.
- Adopt rules to mitigate risk, support a security governance framework, and safeguard state agency digital assets, data, information, and IT resources[27] to ensure availability, confidentiality, and integrity.
- Designate a chief information security officer (CISO) who must develop, operate, and oversee state technology systems' cybersecurity. The CISO must be notified of all confirmed or suspected incidents or threats of state agency IT resources and must report such information to the CIO and the Governor.
- Develop and annually update a statewide cybersecurity strategic plan that includes security goals and objectives for cybersecurity, including the identification and mitigation of risk, proactive protections against threats, tactical risk detection, threat reporting, and response and recovery protocols for cyber incidents.
- Develop a cybersecurity governance framework and publish it for state agency use.
- Assist state agencies in complying with the State Cybersecurity Act.
- Train state agency information security managers and computer security incident response team members, in collaboration with the Florida Department of Law Enforcement (FDLE) Cybercrime Office, on issues relating to cybersecurity, including cybersecurity threats, trends, and best practices.
- Provide cybersecurity training to all state agency technology professionals that develop, assess, and document competencies by role and skill level. The training may be provided in collaboration with the Cybercrime Office, a private sector entity, or an institution of the state university system.
- Annually review state agencies' strategic and operational cybersecurity plans.
- Track, in coordination with agency inspectors general, state agencies' implementation of remediation plans.
- Operate and maintain a Cybersecurity Operations Center led by the CISO to serve as a clearinghouse for threat information and to coordinate with the FDLE to support state agency response to cybersecurity incidents.
- Lead an Emergency Support Function under the state comprehensive emergency management plan.

[24] Section 282.318, F.S.
[25] "Cybersecurity" means the protection afforded to an automated information system in order to attain the applicable objectives of preserving the confidentiality, integrity, and availability of data, information, and information technology resources. Section 282.0041(8), F.S.
[26] Section 282.318(3), F.S.
[27] "Information technology resources" means data processing hardware and software and services, communications, supplies, personnel, facility resources, maintenance, and training. Section 282.0041(22), F.S.

The State Cybersecurity Act requires the head of each state agency to designate an information security manager to administer the cybersecurity program of the state agency.[28] In addition, agency heads must:

- Establish an agency cybersecurity incident response team, which must report any confirmed or suspected cybersecurity incidents to the CISO.
- Submit an annual strategic and operational cybersecurity plan to the DMS.
- Conduct a triennial comprehensive risk assessment to determine the security threats to the data, information, and IT resources of the state agency.
- Develop and update internal policies and procedures, including procedures for reporting cybersecurity incidents and breaches to the FLDS and the Cybercrime Office.
- Implement managerial, operational, and technical safeguards and risk assessment remediation plans recommended by the DMS to address identified risks to the data, information, and IT resources of the agency.
- Ensure periodic internal audits and evaluations of the agency's cybersecurity program.
- Ensure that cybersecurity contract requirements of IT and IT resources and services meet or exceed applicable state and federal laws, regulations, and standards for cybersecurity, including the NIST cybersecurity framework.
- Provide cybersecurity awareness training to all state agency employees concerning cybersecurity risks and the responsibility of employees to comply with policies, standards, guidelines, and operating procedures adopted by the state agency to reduce those risks. The training may be provided in collaboration with the Cybercrime Office, a private sector entity, or an institution of the state university system.
- Develop a process, consistent with FLDS rules and guidelines, to detect, report, and respond to threats, breaches, or cybersecurity incidents.

Florida Cybersecurity Advisory Council

The Florida Cybersecurity Advisory Council (Advisory Council) within the DMS[29] protects IT resources from cyber threats and incidents.[30] The Advisory Council must assist the FLDS with the implementation of best cybersecurity practices, taking into consideration the final recommendations of the Florida Cybersecurity Task Force – a task force created to review and assess the state's cybersecurity infrastructure, governance, and operations.[31] The Advisory Council meets at least quarterly to:[32]

- Review existing state agency cybersecurity policies.
- Assess ongoing risks to state agency IT.
- Recommend a reporting and information sharing system to notify state agencies of new risks.
- Recommend data breach simulation exercises.

[28] Section 282.318(4)(a), F.S.
[29] Section 282.319(1), F.S.
[30] Section 282.319(2), F.S.
[31] Section 282.319(3), F.S. The Cybersecurity Task Force is no longer active. *See*, Florida DMS, *Cybersecurity Task Force Overview*, https://www.dms.myflorida.com/other_programs/cybersecurity_advisory_council/cybersecurity_task_force (last visited Mar. 14, 2023).
[32] Section 282.319(9), F.S.

- Develop cybersecurity best practice recommendations for state agencies, including continuous risk monitoring, password management, and protecting data in legacy and new systems.
- Examine inconsistencies between state and federal law regarding cybersecurity.

Beginning June 30, 2022, and each June 30 thereafter, the Advisory Council must submit cybersecurity recommendations to the Legislature.[33]

III. Effect of Proposed Changes:

The bill bans the use of prohibited applications on devices issued to an employee or officer by a public employer, or otherwise used on a network that is owned, operated, or maintained by a public employer.

Section 1 creates s. 112.22, F.S., to require the Department of Management Services (DMS) to create and maintain a list of prohibited applications of any Internet application that it deems 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. A "prohibited application" is alternatively defined as any that participates in certain activities, such as conducting cyber-espionage against a public employer, and that is created, maintained, or owned by a foreign principal.

The DMS must adopt this list of prohibited applications through rulemaking, publish the list on its website, and disseminate it to public employers.

A foreign principal includes only the following:
- The government or any official of the government of a foreign country of concern;
- A political party or member of a political party in a foreign country of concern;
- A partnership, association, corporation, organization, or other 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 subsidiary thereof; or
- Any person domiciled in a foreign country of concern who is not a citizen of the United States.

Public employers must:
- Block access to any prohibited application via their wireless networks and virtual private networks;
- Restrict access to any prohibited application on any government cell phone, laptop, desktop computer, tablet computer, or other electronic device that can connect to the Internet that has been issued to an employee or officer for a work-related purpose; and
- Retain the ability to remotely wipe and uninstall any prohibited application from any such device that is believed to have been adversely impacted by a prohibited application.

Additionally, the bill prohibits all persons from downloading or accessing any prohibited application on a government-issued device. However, officers and employees may procure a

[33] Section 282.319(11), F.S.

waiver to access a prohibited application from the DMS. Law enforcement officers are wholly exempted from the applications ban if their use of the application is necessary to protect the public safety or to conduct an investigation.

The bill requires an employee or officer to remove any prohibited application from his or her government-issued device within 15 days of the DMS' publication of its list of prohibited applications, and within 15 days of any subsequent update to the list of prohibited applications.

The bill grants the DMS rulemaking authority to administer these provisions. Specifically, the DMS is vested with emergency rulemaking authority to adopt the list of prohibited applications into rule. The DMS's determination of a prohibited application must be on the basis of an application's engagement in specific activities, or on the basis of the presentation of a security risk in the form of unauthorized access to or temporary unavailability of the state's digital assets, systems, networks, servers, or information.

The bill also grants the DMS authority to adopt rules that specify the waiver process, which must require all of the following:

- A description that the employee or officer will conduct, and the state interest that is furthered by the activity;
- The maximum number of government-issued devices and employees or officers to which the waiver will apply;
- The length of time necessary for the waiver, which cannot exceed 1 year (but may be extended through another waiver);
- Risk mitigation strategies that will be instituted to protect state systems, networks, and servers from malicious activity; and
- A description of the circumstances under which the waiver applies.

Section 2 provides a declaration of an important state interest that its information technology resources be protected from security breaches.

Section 3 provides that the bill will take effect on July 1, 2023.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

Article VII, s. 18(a) of the State Constitution provides, in pertinent part, that "no county or municipality shall be bound by any general law requiring such county or municipality to spend funds or take an action requiring the expenditure of funds unless the legislature has determined that such law fulfills an important state interest and unless:"

- The law requiring such expenditure is approved by two-thirds of the membership in each house of the legislature; or
- The expenditure is required to comply with a law that applies to all persons similarly situated, including state and local governments.

The bill requires a county or municipality to take certain actions regarding the security of its IT network and government-issued devices. To comply with this law, the county or

municipality may be required to spend funds. The bill applies to all similarly situated governmental agencies that have IT networks and issue devices, including state agencies, counties, municipalities, special districts, school districts, universities, and colleges. At this time, the bill does not include a legislative finding that the bill fulfills an important state interest. The bill may not be binding on counties and municipalities unless the bill exempt from the mandates requirements because the overall fiscal impact is insignificant.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

D. State Tax or Fee Increases:

None.

E. Other Constitutional Issues:

The Legislature may not delegate its constitutional duties to another branch of government.[34] While the Legislature must make fundamental policy decisions, it may delegate the task of implementing that policy to executive agencies with "some minimal standards and guidelines ascertainable by reference to the enactment establishing the program."[35] Moreover, the Legislature can permit "administration of legislative policy by an agency with the expertise and flexibility to deal with complex and fluid conditions."[36]

Florida courts have found an unlawful delegation of legislative authority in the following instances:

- Where the Legislature allowed the Department of State to "in its discretion allow such a candidate to withdraw…";[37] and
- Where the Legislature created a criminal penalty for escape from certain classifications of juvenile detention facilities, but delegated the classification (or determination whether to classify at all) to an agency.[38]

Comparatively, the Legislature's delegation of rulemaking authority to the Florida Game and Freshwater Fish Commission (FWC) to implement the Legislature's ban on owning wildlife was deemed a proper delegation. The Legislature's provision of a statutory definition of the term "wildlife' as those animals that posed a "real or potential threat to

[34] *See* FLA. CONST. art. II, s. 3.
[35] *Askew v. Cross Key Waterways*, 372 So.2d 913, 925 (Fla. 1978).
[36] *Microtel, Inc. v. Fla. Public Serv. Comm'n.*, 464 So.2d 1189, 1191 (Fla. 1991).
[37] *Fla. Dep't. of State, Div. of Elections v. Martin*, 916 So.2d 763 (Fla. 2005).
[38] *D.P. v. State*, 597 So.2d 952 (Fla. 1st DCA, 1992)(disapproved on other grounds).

human safety" provided sufficient confines to the FWC's duty to further define the term by rulemaking.[39]

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

None.

C. Government Sector Impact:

The DMS will be required to conduct research into a large number of existing applications offered to create a list of prohibited applications. This will be an ongoing effort, as new applications are created and offered daily.

Additionally, the DMS will be required to create rules associated with the implementation of this bill, in particular to provide agency procedures regarding the waiver process, and to create and update the list of prohibited applications.

State agencies and local government entities may incur indeterminate costs to comply with the provisions of this bill.

VI. Technical Deficiencies:

None.

VII. Related Issues:

There is no penalty stated in the bill; however, an employer may fire an employee on the basis of his or her violation of law.

The bill provides for a waiver process, administered by the DMS. This will result in government entities creating, and the DMS holding specific information that could reveal what government employees are using a prohibited application, and which may explain their purpose for the use. If this information were obtained for insidious purposes, the government user's legitimate purpose could be undermined, and the user could be targeted for data mining or other illegitimate purposes.

[39] *State v. Cumming*, 365 So.2d. 153, 155 (Fla. 1978). While the Court further found the Legislature's delegation of wildlife permitting authority to the FWC to be an appropriate delegation of authority, they overturned the particular application of the law because the rules adopted by the FWC were overbroad and vague, so a reasonable purchaser could not reasonably interpret the guidelines applied to them.

VIII. Statutes Affected:

112.22
This bill creates section 112.22, F.S.

IX. Additional Information:

A. Committee Substitute – Statement of Substantial Changes:
(Summarizing differences between the Committee Substitute and the prior version of the bill.)

CS by Governmental Oversight and Accountability on March 15, 2023:

- Defines a prohibited application as one that poses a security risk, either on the basis of specific activities, or as a result of a finding by the DMS, based on the application's risk of unauthorized access to or temporary unavailability of the public employer's records, digital assets, systems, networks, servers, or information;
- Prohibits any person, not just employees, from downloading or accessing a prohibited application on a government-issued device;
- Provides emergency rulemaking authority to the DMS to institute a rule that identifies prohibited applications, and general rulemaking authority to update it thereafter;
- Requires the DMS to update the list of prohibited applications at least quarterly, and to distribute it to public employers;
- Allows officers or employees of a public employer 15 days from the publication or provision of an update of the DMS' list of prohibited applications to comply therewith;
- Specifies certain requirements that the DMS must incorporate into its waiver process; and
- Replaces the term "employee" with "officer and employee" and "governmental entity or public education institution" with "public employer," which includes schools, local governments, state agencies, and charter school governing boards.

B. Amendments:

None.