HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: CS/CS/HB 563 Applications on Government Devices
SPONSOR(S): State Administration & Technology Appropriations Subcommittee, Constitutional Rights, Rule of Law & Government Operations Subcommittee, Amesty and others
TIED BILLS: **IDEN./SIM. BILLS:** CS/CS/SB 258

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR or BUDGET/POLICY CHIEF
1) Constitutional Rights, Rule of Law & Government Operations Subcommittee	15 Y, 0 N, As CS	Villa	Miller
2) State Administration & Technology Appropriations Subcommittee	14 Y, 0 N, As CS	Mullins	Topp
3) State Affairs Committee			

SUMMARY ANALYSIS

Certain technology companies headquartered or incorporated in foreign countries of concern are under increasing scrutiny by the U.S. government as a potential privacy and security risk to U.S. citizens. This is because technology companies that do business in foreign countries of concern, like China or Russia, are subject to those countries' laws and are typically required to turn over user data, intellectual property, and proprietary business information when requested by the foreign government.

The bill requires the Department of Management Services (DMS) to create a list of prohibited applications, defined as those determined by DMS to present a security risk in the form of unauthorized access to or temporary unavailability of a public employer's information technology resources; or those that are created, maintained, or owned by a foreign principal and that engage in specific activities that endanger cybersecurity. This definition will likely include social media applications like TikTok and WeChat.

The bill requires public employers (including state agencies, public education institutions, and local governments) to block or restrict access to prohibited applications on their networks and devices. The bill also requires public employers to retain the ability to remotely wipe and uninstall prohibited applications from a compromised government-issued device.

The bill prohibits all persons from downloading prohibited applications on government-issued devices, and requires public officers and employees to remove any prohibited application from their government devices within 15 calendar days after DMS publishes or updates the prohibited applications list. DMS must notify public employers when it updates the prohibited applications list.

The bill authorizes a law enforcement officer to use a prohibited application if the use is necessary to protect the public safety or to conduct an investigation. The bill also allows other government employees to use a prohibited application if they are granted a waiver by DMS. The request for a waiver must include certain information.

The bill provides emergency rulemaking authority to DMS to adopt the prohibited applications list, and express rulemaking authority to implement the act.

The bill will likely have an indeterminate, negative fiscal impact on state and local government expenditures. However, it is anticipated that DMS can absorb the workload within existing resources. *See* Fiscal Analysis section.

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

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 its 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, internet addresses, 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 and similar 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 requiring companies that operate in the country to turn over user data, intellectual property, and proprietary business information when requested 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

[1] Datareportal.com, *TikTok Statistics and Trends*, https://datareportal.com/essential-tiktok-stats (last visited March 19, 2023).
[2] ByteDance, Inc., *About Us*, https://www.bytedance.com/en/ (last visited March 19, 2023); *see also*, Newsweek, Chloe Mayer, *Is TikTok Owned by the Chinese Communist Party?*, https://www.newsweek.com/tiktok-owned-controlled-china-communist-party-ccp-influence-1752415 (last visited March 19, 2023).
[3] Congressional Research Service, Patricia Moloney Figliola, *TikTok: Technology Overview and Issues*, https://crsreports.congress.gov/product/pdf/R/R46543 (last visited March 19, 2023).
[4] Business of Apps, Mansoor Iqbal, *WeChat Revenue and Usage Statistics (2022)*, https://www.businessofapps.com/data/wechat-statistics/ (last visited March 19, 2023).
[5] *See* WeChat, *WeChat Privacy Policy*, https://www.wechat.com/en/privacy_policy.html (last visited March 19, 2023).
[6] *See* 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*, 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 March 19, 2023).
[7] Nazak Nikakhtar, U.*S. Businesses Must Navigate Significant Risk of Chinese Government Access to Their Data*, https://www.jdsupra.com/legalnews/u-s-businesses-must-navigate-3014130/ (last visited March 19, 2023).
[8] Reuters, Echo Wang and David Shepardson, *TikTok moves U.S. user data to Oracle servers*, https://www.reuters.com/technology/tiktok-moves-us-user-data-oracle-servers-2022-06-17/ (last visited March 19, 2023).
[9] Forbes, Emily Baker-White, *Exclusive: TikTok Spied on Forbes Journalists*, https://www.forbes.com/sites/emilybaker-white/2022/12/22/tiktok-tracks-forbes-journalists-bytedance/?sh=3bd5d3327da5 (last visited March 19, 2023).
[10] AP News, Haleluya Hadero, *Why TikTok is Being Banned on Government Phones in US and Beyond* https://apnews.com/article/why-is-tiktok-being-banned-7d2de01d3ac5ab2b8ec2239dc7f2b20d (last visited March 19, 2023).
[11] President Donald J. Trump, *Executive Order on Addressing the Threat Posed by TikTok*, https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/ (last visited March 19, 2023).

TikTok's U.S.-arm.[12] President Trump also took similar action banning 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.[14]

Congress passed the "No TikTok on Government Devices Act" as part of the omnibus spending bill in December 2022.[15] 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 information technology (IT)[16] to remove and disallow installations of TikTok within 30 days.[17] The guidance allows exceptions to the use and installation ban for the purposes of law enforcement activities, national security interests and activities, and security research.

As of January 2023, at least 32 states have acted to ban the use of high-risk software and services on state devices or networks.[18]

On August 11, 2020, the Chief Financial Officer of Florida signed a directive banning TikTok on devices issued by the Department of Financial Services.[19] In addition, on March 7, 2023, the Miami-Dade County Commission voted to ban TikTok from its county's work phones.[20]

State and Local IT Management and Cybersecurity

The Department of Management Services (DMS) oversees IT governance and cybersecurity for the executive branch of State government,[21] and provides cybersecurity training and services to local governmental entities.[22] The Florida Digital Service (FLDS) within DMS was established by the Legislature in 2020;[23] the head of FLDS is appointed by the Secretary of DMS and serves as the state chief information officer (CIO).[24] The CIO designates the state chief information security officer, who is responsible for the development, operation, and oversight of cybersecurity for state technology systems and receives cybersecurity incident reports from state and local governments.[25]

The FLDS was created to modernize state government technology and information services.[26] Accordingly, DMS, through FLDS, has the following powers, duties, and functions:

- Develop IT policy for the management of the state's IT resources;

[12] President Donald J. Trump, *Executive Order Regarding the Acquisition of Musical.ly by ByteDance Ltd.*, https://home.treasury.gov/system/files/136/EO-on-TikTok-8-14-20.pdf. (last visited March 19, 2023).
[13] President Donald J. Trump, *Executive Order on Addressing the Threat Posed by WeChat*, https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-posed-wechat/ (last visited March 19, 2023).
[14] The New York Times, Katie Rodgers and Cecilia Kang, *Biden Revokes and Replaces Trump Order that Banned TikTok*, https://www.nytimes.com/2021/06/09/us/politics/biden-tiktok-ban-trump.html (last visited March 19, 2023).
[15] Pub. L. No. 117-328, div. R, §§101-102.
[16] "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).
[17] Office of Management and Budget, *Memorandum: No TikTok on Government Devices Implementation Guidance*, https://www.whitehouse.gov/wp-content/uploads/2023/02/M-23-13-No-TikTok-on-Government-Devices-Implementation-Guidance_final.pdf (last visited March 19, 2023).
[18] CNN Business, Brian Fang and Christopher Hickey, *TikTok access from Government Devices now Restricted in More than Half of US States*, https://www.cnn.com/2023/01/16/tech/tiktok-state-restrictions/index.html (last visited March 19, 2023).
[19] Florida Department of Financial Services, *Chief Financial Officer Directive 2020-14*, https://myfloridacfo.com/docs-sf/cfo-news-libraries/news-documents/2020/cfo-directive-2020-14.pdf?sfvrsn=8e4c2283_2 (last visited March 19, 2023).
[20] NBC Miami, Heather Walker, *Miami-Dade Commissioners Vote to Ban TikTok on County Devices*, https://www.nbcmiami.com/news/local/miami-dade-commissioners-vote-to-ban-tiktok-on-county-devices/2988107/ (last visited March 19, 2023).
[21] S. 282.0051, F.S.
[22] S. 212.3185, F.S. "Local government" means any county or municipality. S. 282.3185(2), F.S.
[23] Ch. 2020-161, Laws of Fla.
[24] S. 282.0051(2)(a), F.S.
[25] Ss. 282.318(3)(c), F.S. and 282.3185(5), F.S.
[26] S. 282.0051(1), F.S.

- 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[27]
- Standardize and consolidate IT services that support interoperability, Florida's cloud first policy, and other common business functions and operations.

Foreign Countries of Concern

Federal law imposes many layers of scrutiny on certain dealings with foreign nationals, mostly related to science and technology having military implications, sales of arms and certain financial transactions related to terrorism, human trafficking, international drug dealing, and other important national interests. Various federal agencies publish lists related to sanctions, restrictions, and scrutiny imposed by federal law. One such list published by the U.S. Department of State is the "state sponsors of terrorism" list that currently includes Cuba, Iran, North Korea, and Syria.[28] In addition, many programs scrutinize transactions involving America's biggest global competitors, the People's Republic of China and Russia. On January 19, 2021, the U.S. Department of Commerce published an interim final rule entitled: Securing the Information and Communications Technology and Services Supply Chain.[29] That interim rule defined "foreign adversaries" to include Russia, the People's Republic of China, the Nicolás Maduro government of Venezuela, Cuba, Iran, and North Korea. This is a relatively short list of scrutinized countries compared to other federal lists of countries scrutinized in various import-export and financial oversight programs.[30] Along with Syria, a state sponsor of terrorism, these reflect the foreign governments most hostile to U.S. interests. The rule became effective on March 22, 2021.[31]

Effect of the Bill

The bill requires DMS to compile and maintain a list of prohibited applications and publish the list on its website. DMS must update the list quarterly and provide notice of any updates to public employers.[32] Within 15 days after DMS issues or updates its prohibited applications list, an employee or officer[33] of a public employer who uses a government-issued[34] device must remove, delete, or uninstall any prohibited applications from his or her government-issued device.

The bill defines "prohibited application" to mean an application that meets the following criteria:

- Any Internet application that is created, maintained, or owned by a foreign principal[35] and that participates in activities that include, but are not limited to:

[27] 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. S. 282.0051(1)(m), F.S.
[28] U.S. Department of State, *State Sponsors of Terrorism*, https://www.state.gov/state-sponsors-of-terrorism/ (last visited March 19, 2023).
[29] 86 Fed. Reg. 4909 (Jan. 19, 2021).
[30] Such lists are published by the Department of Treasury, Office of Foreign Assets Control, Department of Commerce, Bureau of Industry and Security, Department of State, Directorate of Defense Trade Controls, as well as multiple Department of Defense and Department of Energy agencies.
[31] *See supra* note 29; *see also* 15 C.F.R. pt. 7.4 (2021).
[32] The bill defines "public employer" to mean the state or any agency, authority, branch, bureau, commission, department, division, special district, institution, university, institution of higher education, or board thereof; or any county, district school board, charter school governing board, or municipality, or any agency, branch, department, board, or metropolitan planning organization thereof.
[33] The bill defines "employee or officer" to mean a person who performs labor or services for a public employer in exchange for salary, wages, or other remuneration.
[34] The bill defines "government-issued device" to mean a cellular telephone, desktop computer, laptop computer, computer tablet, or other electronic device capable of connecting to the Internet which is owned or leased by a public employer and issued to an employee or officer for work-related purposes.
[35] The bill defines "foreign principal" to mean the government or an official of the government of a foreign country of concern; a political party or a member of a political party or any subdivision of a political party in a foreign country of concern; a partnership, an association, a corporation, an organization, or another 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 thereof; or any person who is domiciled in a foreign country of concern and is neither a citizen nor lawful permanent resident of the United States. The bill defines "foreign country of concern" to mean the People's Republic of China, the Russian Federation, the Islamic Republic of Iran, the Democratic People's Republic of Korea, the Republic of Cuba, the Venezuelan regime of Nicolás Maduro, or the Syrian Arab Republic, including any agency of or any other entity under significant control of such foreign country of concern.

    - Collecting keystrokes or sensitive personal, financial, proprietary, or other business data;
    - Compromising e-mail and acting as a vector for ransomware deployment;
    - Conducting cyber-espionage against a public employer;
    - Conducting surveillance and tracking of individual users; or
    - Using algorithmic modifications to conduct disinformation or misinformation campaigns; or
- Any Internet application the department 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.

The bill requires public employers to do the following:

- Block all prohibited applications from public access on any network and virtual private network that it owns, operates, or maintains;
- Restrict access to any prohibited application on a government-issued device; and
- 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.

The bill prohibits a person, including an employee or officer of a public employer from downloading or accessing any prohibited application on any government-issued device. However, this prohibition does not apply to a law enforcement officer[36] if the use of the prohibited application is necessary to protect the public safety or conduct an investigation within the scope of his or her employment. In addition, a public employer may request a waiver from DMS to allow designated employees or officers to download or access a prohibited application on a government-issued device.

DMS must establish procedures for granting or denying requests for waivers from public employers. However, the bill requires the waiver to include the following information:

- 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 to which the waiver will apply;
- The length of time necessary for the waiver. Any waiver granted must be limited to a timeframe of no more than one year, but DMS may 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 under which the waiver applies.

The bill grants DMS emergency rule-making authority in order to adopt the list of prohibited applications. Such rulemaking must occur initially by filing emergency rules within 30 days after July 1, 2023. In addition, DMS is authorized to adopt any rules necessary to administer the act.

Finally, the bill declares that it fulfills an important state interest.

B. SECTION DIRECTORY:

Section 1 creates s. 112.22, F.S., relating to restrictions and prohibitions for the use of applications from foreign countries of concern.

Section 2 provides that the Legislature finds that the act fulfills an important state interest.

Section 3 provides an effective date of July 1, 2023.

[36] "Law enforcement officer," is defined in s. 943.10(1), F.S., incorporated into the bill, to mean any person who is elected, appointed, or employed full time by any municipality or the state or any political subdivision thereof; who is vested with authority to bear arms and make arrests; and whose primary responsibility is the prevention and detection of crime or the enforcement of the penal, criminal, traffic, or highway laws of the state. This definition includes all certified supervisory and command personnel whose duties include, in whole or in part, the supervision, training, guidance, and management responsibilities of full-time law enforcement officers, part-time law enforcement officers, or auxiliary law enforcement officers but does not include support personnel employed by the employing agency.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

None.

2. Expenditures:

The bill will likely have an indeterminate, negative fiscal impact on state government expenditures. The bill requires DMS to maintain a list of prohibited applications and establish procedures for granting certain waivers. In addition, the bill requires public employers to configure their networks to block or restrict access to prohibited applications. The amount of expenditures required by the bill is indeterminate at this time. However, it is anticipated DMS will absorb any anticipated workload or fiscal impact from within existing resources.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

None.

2. Expenditures:

The bill will likely have an indeterminate, negative fiscal impact on local government expenditures. The bill requires public employers to take certain actions to block or restrict access to prohibited applications. The amount of expenditures required by the bill is indeterminate at this time and may depend on whether a local public employer already has the technology necessary to implement the provisions of the bill.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

None.

D. FISCAL COMMENTS:

None.

III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

The county/municipality mandates provision of Art. VII, s. 18 of the Florida Constitution may apply because this bill requires political subdivisions to take certain actions to block or restrict access to prohibited applications; however, an exemption may apply if the fiscal impact of the bill is insignificant. In addition, an exception may apply because the bill applies to similarly situated state and local governmental entities and the bill provides an important state interest determination.

2. Other:

None.

B. RULE-MAKING AUTHORITY:

The bill grants DMS emergency rule-making authority in order to adopt the list of prohibited applications. Such rulemaking must occur initially by filing emergency rules within 30 days after July 1, 2023. In addition, DMS is authorized to adopt any rules necessary to administer the act.

C. DRAFTING ISSUES OR OTHER COMMENTS:

None.

IV. AMENDMENTS/COMMITTEE SUBSTITUTE CHANGES

On March 22, 2023, the Constitutional Rights, Rule of Law & Government Operations Subcommittee adopted a proposed committee substitute (PCS) and reported the bill favorably as a committee substitute. The PCS differed from the bill in that it:

- Requires DMS to create a list of prohibited applications that present a security risk to public employers;
- Requires public employers to block all prohibited applications on their devices and networks;
- Requires public officers and employees to remove prohibited applications from their government issued devices within a certain time;
- Authorizes a law enforcement officer to use a prohibited application under certain circumstances;
- Authorizes other public employers to request a waiver from DMS to use a prohibited application; and
- Requires the waiver request to contain specified information.

On April 12, 2023, the State Administration and Technology Appropriations Subcommittee adopted an amendment and reported the bill favorably. The amendment changed the part of the definition of "foreign principal" relating to any person who is domiciled in a foreign country of concern and is not a citizen or a lawful permanent resident of the United States, to any person who is domiciled in a foreign country of concern and is neither a citizen nor lawful permanent resident of the United States.

This analysis is drawn to the committee substitute as adopted by the State Administration and Technology Appropriations Subcommittee.