SENATE BILL 83:
No High Risk Apps/Gov't Networks & Devices.

2023-2024 General Assembly

Committee:	Senate Rules and Operations of the Senate	**Date:**	March 8, 2023
Introduced by:	Sens. Moffitt, Perry, Hanig	**Prepared by:**	Kristen L. Harris
Analysis of:	Third Edition		Staff Attorney

OVERVIEW: Senate Bill 83 would do all of the following:

- ***Prohibit a public agency, the judicial branch, and the legislative branch from:***
  - ***Allowing the use of any high risk platform on that public agency's or branch's network.***
  - ***Allowing an employee, elected official, or appointee from installing, using, or otherwise accessing a high risk platform on a device owned, leased, maintained, or otherwise controlled by that public agency or branch. This prohibition would apply to a student at a public agency.***
- ***Require each public agency, the judicial branch, and the legislative branch to adopt a policy governing the use of networks and the use of high risk platforms.***
- ***Create exemptions for officials or employees engaged in certain activities in the course of their official duties and require the State Chief Information Officer to publish recommendations for the exemptions by April 15, 2023.***
- ***Require any employee, elected official, appointee, or student covered by this act to remove, delete, or uninstall the high risk platform on a covered device by April 15, 2023.***

CURRENT LAW:

Criminal Law Provisions

G.S. 14-456 provides: "Any person who willfully and without authorization denies or causes the denial of computer, computer program, computer system, or computer network services to an authorized user of the computer, computer program, computer system, or computer network services is guilty of a Class 1 misdemeanor."

G.S. 14-456.1 provides: "Any person who willfully and without authorization denies or causes the denial of government computer services is guilty of a Class H felony."

Executive Branch Prohibitions on the use of TikTok and WeChat

On January 12, 2023, Governor Cooper issued Executive Order No. 276 directing the State Chief Information Officer (CIO) and Department of Information Technology (DIT) to develop a policy that prohibited the use of TikTok and WeChat on State agency information technology systems.

Effective January 26, 2023, DIT and the CIO issued: "Use of High Risk Applications, Version 1.0." The policy identified TikTok and WeChat as High-Risk Applications and provided that: (1) State agency employees may not install or otherwise utilize the identified High-Risk Applications on State-issued devices and must remove any existing instances of the TikTok and WeChat applications from State-issued

devices; (2) State agency employees may not access any High-Risk Technology website on a State-issued device; (3) The State Network may not be used to access High-Risk Technology on any personally owned device; (4) State agencies and their employees may obtain an exception from the prohibition on the installation and use of High-Risk Applications for law enforcement or other legitimate purposes under conditions specified by DIT. The policy applies to devices owned by or issued by State agencies and personal devices that are connected to the State network.

State agencies and State agency employees must comply with the policy within 60 days of its enactment.

BILL ANALYSIS: Senate Bill 83 would do the following:

- Define "high risk platforms" to include (1) "TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited"; (2) "WeChat or any successor application or service developed or provided by Tencent Holdings Limited or an entity owned by Tencent Holdings Limited"; and (3) "Telegram or any successor application or service developed or provided by Telegram FZ LLC or an entity owned by Telegram FZ LLC."
- Define "public agency" to include: "All agencies and constitutional officers of the State, including all boards, departments, divisions, constituent institutions of The University of North Carolina, community colleges, and other units of government in the executive branch"; units of local government; public authorities; and public school units.
- Prohibit public agencies, the judicial branch, and the legislative branch from allowing the use of any high risk platform on that public agency's or branch's network.
- Prohibit public agencies, the judicial branch, and the legislative branch from allowing an employee, elected official, or appointee to install, use, or otherwise access a high risk platform on a device owned, leased, maintained, or otherwise controlled by that public agency or branch. This prohibition would also apply to students of public agencies. There would be an exemption for cities that provide internet services to its citizens as a public enterprise.
- Create exceptions for officials or employees engaging in any of the following activities during that official's or employee's official duties:
    - Investigating or prosecuting crimes.
    - Identifying potential security or cybersecurity threats.
    - Protecting human life.
    - Establishing, testing, and maintaining firewalls, protocols, and otherwise implementing this section.
    - Participating in judicial or quasi-judicial proceedings.
    - Conducting or participating in an externally-funded research project at one of the constituent institutions of The University of North Carolina.

  The State Chief Information Officer would be required to publish recommendations for appropriate access to high risk platforms no later than April 15, 2023.
- Require each public agency, the judicial branch, and the legislative branch, no later than July 1, 2023, to adopt a policy governing the use of networks and the use of high risk platforms on devices owned, leased, maintained, or otherwise controlled by that public agency or branch.

- Require public agencies to report information no later than August 1 of each year to the State Chief Information Officer on incidences of unauthorized uses and attempted uses of a high risk platform and require the State Chief Information Officer to report this information to the Joint Legislative Oversight Committee on Information Technology no later than October 1 of each year.
- Require employees, elected officials, appointees, and students of a public agency with a high risk platform on a device owned, leased, maintained, or otherwise controlled by that public agency to remove, delete, or uninstall the high risk platform no later than April 15, 2023. This provision would also apply to the judicial and legislative branches.
- Provide that denial of access to a high risk platform does not violate criminal law provisions prohibiting the denial of computer services and government computer services to authorized users.

EFFECTIVE DATE: The act would become effective April 1, 2023

BACKGROUND: The United States Congress passed its own ban on the use of TikTok for federal executive agencies and directed the Office of Management and Budget to develop standards and guidelines for federal executive agencies requiring removal of the application. (Public Law No 117-328). In addition to North Carolina's Executive Order No. 276, at least 18 other states' governors have taken similar actions. At least, 23 states have proposed legislation.

** Brad Krehely and Erika Churchill, Legislative Analysis, contributed to this summary.*