GENERAL ASSEMBLY OF NORTH CAROLINA
SESSION 2023

SENATE BILL 83
State and Local Government Committee Substitute Adopted 2/21/23

Short Title: No High Risk Apps/Gov't Networks & Devices. (Public)

Sponsors:

Referred to:

February 9, 2023

A BILL TO BE ENTITLED

AN ACT REGARDING THE USE OF HIGH RISK PLATFORMS ON GOVERNMENT NETWORKS AND GOVERNMENT DEVICES.

The General Assembly of North Carolina enacts:

SECTION 1.(a) Article 84 of Chapter 143 of the General Statutes is amended by adding a new section to read:

"**§ 143-805. High risk platforms on government networks and devices.**

(a) Notwithstanding G.S. 14-456 and G.S. 14-456.1, a public agency shall not permit the use of any high risk platform on a network of that public agency. Notwithstanding G.S. 14-456 and G.S. 14-456.1, the judicial branch shall not permit the use of any high risk platform on a network of the judicial branch. Notwithstanding G.S. 14-456 and G.S. 14-456.1, the legislative branch shall not permit the use of any high risk platform on a network of the legislative branch.

(b) Notwithstanding G.S. 14-456 and G.S. 14-456.1, no public agency shall permit an employee, elected official, or appointee of that public agency to install, use, or otherwise access a high risk platform on a device owned, leased, maintained, or otherwise controlled by that public agency. No public agency shall permit a student of that public agency to install, use, or otherwise access a high risk platform on a device owned, leased, maintained, or otherwise controlled by that public agency. The judicial branch shall not permit an employee, elected official, or appointee of the judicial branch to install, use, or otherwise access a high risk platform on a device owned, leased, maintained, or otherwise controlled by the judicial branch. The legislative branch shall not permit an employee, elected official, or appointee of the legislative branch to install, use, or otherwise access a high risk platform on a device owned, leased, maintained, or otherwise controlled by the legislative branch.

(c) Each public agency shall adopt a policy governing the use of its network and the use of high risk platforms on devices owned, leased, maintained, or otherwise controlled by that public agency. The judicial and legislative branches shall adopt a policy governing the use of that branch's networks and the use of high risk platforms on devices owned, leased, maintained, or otherwise controlled by those branches.

(d) Subsection (b) of this section shall not apply to an official or employee that is engaged in any of the following activities in the course of that official's or employee's official duties:

(1) Investigating or prosecuting crimes.
(2) Identifying potential security or cybersecurity threats.
(3) Protecting human life.
(4) Establishing, testing, and maintaing firewalls, protocols, and otherwise implementing this section.
(5) Participating in judicial or quasi-judicial proceedings.

(e) This section shall not apply to the user of an authorized account paying for use of communications services under Article 16A of Chapter 160A of the General Statutes, including those communications services exempted under G.S. 160A-340.2(b) or (c).

(f) Annually, no later than August 1 and in the format required by the Chief Information Officer, each public agency shall report information to the Chief Information Officer on the number of incidences of unauthorized uses and attempted uses of a high risk platform on that public agency's network; whether or not those unauthorized uses were by an employee, elected official, appointee, or student of that public agency; and whether or not any of those unauthorized uses were on a device owned, leased, maintained, or otherwise controlled by that public agency. Annually, no later than October 1, the Chief Information Officer shall compile and report to the Joint Legislative Oversight Committee on Information Technology the information submitted in accordance with this subsection.

(g) The following definitions apply in this section:

(1) Device. – Any cellular phone, desktop or laptop computer, or other electronic equipment capable of connecting to a network.

(2) High risk platform. – The following applications, websites, and other products that pose an unacceptable level of cybersecurity threat to data:

a. TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited.

b. WeChat or any successor application or service developed or provided by Tencent Holdings Limited or an entity owned by Tencent Holdings Limited.

c. Telegram or any successor application or service developed or provided by Telegram FZ LLC or an entity owned by Telegram FZ LLC.

(3) Network. – Any of the following, whether through owning, leasing, maintaining, or otherwise controlling:

a. The interconnection of communication systems with a computer through remote or local terminals, or a complex consisting of two or more interconnected computers or telephone switching equipment.

b. Internet service.

c. Internet access.

(4) Public agency. – Any of the following:

a. 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.

b. Units of local government as defined in G.S. 159-7.

c. Public authorities as defined in G.S. 159-7.

d. Public school units as defined in G.S. 115C-5."

SECTION 1.(b) Any employee, elected official, or appointee of a public agency with a high risk platform on a device owned, leased, maintained, or otherwise controlled by that public agency shall remove, delete, or uninstall the high risk platform no later than April 15, 2023. Any student of a public agency with a high risk platform on a device owned, leased, maintained, or otherwise controlled by that public agency shall remove, delete, or uninstall the high risk platform no later than April 15, 2023. Any employee, elected official, or appointee of the judicial or legislative branches with a high risk platform on a device owned, leased, maintained, or otherwise controlled by that branch shall remove, delete, or uninstall the high risk platform no later than April 15, 2023.

SECTION 2.(a) G.S. 14-456 is amended by adding a new subsection to read:

"(c) This section shall not apply to denial of high risk platforms as required by G.S. 143-805."

SECTION 2.(b) G.S. 14-456.1 is amended by adding a new subsection to read:

"(c) This section shall not apply to denial of high risk platforms as required by G.S. 143-805."

SECTION 3. The Chief Information Officer shall publish recommendations for appropriate access to high risk platforms for the purposes authorized by G.S. 143-805(d), as enacted by this act, no later than April 15, 2023.

SECTION 4. Each public agency, the judicial branch, and legislative branch shall adopt the policy required by G.S. 143-805(c), as enacted by this act, no later than July 1, 2023.

SECTION 5. This act becomes effective April 1, 2023.