

GENERAL ASSEMBLY OF NORTH CAROLINA
SESSION 2023

S

3

SENATE BILL 83
State and Local Government Committee Substitute Adopted 2/21/23
Judiciary Committee Substitute Adopted 3/7/23

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

(Public)

Sponsors:

Referred to:

February 9, 2023

1 A BILL TO BE ENTITLED
2 AN ACT REGARDING THE USE OF HIGH RISK PLATFORMS ON GOVERNMENT
3 NETWORKS AND GOVERNMENT DEVICES.

4 The General Assembly of North Carolina enacts:

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

7 **"§ 143-805. High risk platforms on government networks and devices.**

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

13 (b) Notwithstanding G.S. 14-456 and G.S. 14-456.1, no public agency shall permit an
14 employee, elected official, or appointee of that public agency to install, use, or otherwise access
15 a high risk platform on a device owned, leased, maintained, or otherwise controlled by that public
16 agency. Notwithstanding G.S. 14-456 and G.S. 14-456.1, no public agency shall permit a student
17 of that public agency to install, use, or otherwise access a high risk platform on a device owned,
18 leased, maintained, or otherwise controlled by that public agency. Notwithstanding G.S. 14-456
19 and G.S. 14-456.1, the judicial branch shall not permit an employee, elected official, or appointee
20 of the judicial branch to install, use, or otherwise access a high risk platform on a device owned,
21 leased, maintained, or otherwise controlled by the judicial branch. Notwithstanding G.S. 14-456
22 and G.S. 14-456.1, the legislative branch shall not permit an employee, elected official, or
23 appointee of the legislative branch to install, use, or otherwise access a high risk platform on a
24 device owned, leased, maintained, or otherwise controlled by the legislative branch.

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

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

- 32 (1) Investigating or prosecuting crimes.
33 (2) Identifying potential security or cybersecurity threats.
34 (3) Protecting human life.



- 1 (4) Establishing, testing, and maintaining firewalls, protocols, and otherwise
2 implementing this section.
- 3 (5) Participating in judicial or quasi-judicial proceedings.
- 4 (6) Conducting or participating in an externally funded research project at one of
5 the constituent institutions of The University of North Carolina.
- 6 (e) This section shall not apply to the user of an authorized account paying for use of
7 communications services under Article 16A of Chapter 160A of the General Statutes, including
8 those communications services exempted under G.S. 160A-340.2(b) or (c).
- 9 (f) Annually, no later than August 1 and in the format required by the State Chief
10 Information Officer, each public agency shall report information to the State Chief Information
11 Officer on the number of incidences of unauthorized uses and attempted uses of a high risk
12 platform on that public agency's network; whether or not those unauthorized uses were by an
13 employee, elected official, appointee, or student of that public agency; and whether or not any of
14 those unauthorized uses were on a device owned, leased, maintained, or otherwise controlled by
15 that public agency. Annually, no later than October 1, the State Chief Information Officer shall
16 compile and report to the Joint Legislative Oversight Committee on Information Technology the
17 information submitted in accordance with this subsection.
- 18 (g) The following definitions apply in this section:
- 19 (1) Device. – Any cellular phone, desktop or laptop computer, or other electronic
20 equipment capable of connecting to a network.
- 21 (2) High risk platform. – The following applications, websites, and other products
22 that pose an unacceptable level of cybersecurity threat to data:
- 23 a. TikTok or any successor application or service developed or provided
24 by ByteDance Limited or an entity owned by ByteDance Limited.
- 25 b. WeChat or any successor application or service developed or provided
26 by Tencent Holdings Limited or an entity owned by Tencent Holdings
27 Limited.
- 28 c. Telegram or any successor application or service developed or
29 provided by Telegram FZ LLC or an entity owned by Telegram FZ
30 LLC.
- 31 (3) Network. – Any of the following, whether through owning, leasing,
32 maintaining, or otherwise controlling:
- 33 a. The interconnection of communication systems with a computer
34 through remote or local terminals, or a complex consisting of two or
35 more interconnected computers or telephone switching equipment.
- 36 b. Internet service.
- 37 c. Internet access.
- 38 (4) Public agency. – Any of the following:
- 39 a. All agencies and constitutional officers of the State, including all
40 boards, departments, divisions, constituent institutions of The
41 University of North Carolina, community colleges, and other units of
42 government in the executive branch.
- 43 b. Units of local government as defined in G.S. 159-7.
- 44 c. Public authorities as defined in G.S. 159-7.
- 45 d. Public school units as defined in G.S. 115C-5."

46 **SECTION 1.(b)** Any employee, elected official, or appointee of a public agency
47 with a high risk platform on a device owned, leased, maintained, or otherwise controlled by that
48 public agency shall remove, delete, or uninstall the high risk platform no later than April 15,
49 2023. Any student of a public agency with a high risk platform on a device owned, leased,
50 maintained, or otherwise controlled by that public agency shall remove, delete, or uninstall the
51 high risk platform no later than April 15, 2023. Any employee, elected official, or appointee of

1 the judicial or legislative branches with a high risk platform on a device owned, leased,
2 maintained, or otherwise controlled by that branch shall remove, delete, or uninstall the high risk
3 platform no later than April 15, 2023.

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

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

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

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

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

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

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