

117TH CONGRESS
1ST SESSION

H. R. 2685

IN THE SENATE OF THE UNITED STATES

DECEMBER 2, 2021

Received; read twice and referred to the Committee on Commerce, Science,
and Transportation

AN ACT

To direct the Assistant Secretary of Commerce for Communications and Information to submit to Congress a report examining the cybersecurity of mobile service networks, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Understanding Cyber-
3 security of Mobile Networks Act”.

4 **SEC. 2. REPORT ON CYBERSECURITY OF MOBILE SERVICE**
5 **NETWORKS.**

6 (a) IN GENERAL.—Not later than 1 year after the
7 date of the enactment of this Act, the Assistant Secretary,
8 in consultation with the Department of Homeland Secu-
9 rity, shall submit to the Committee on Energy and Com-
10 merce of the House of Representatives and the Committee
11 on Commerce, Science, and Transportation of the Senate
12 a report examining the cybersecurity of mobile service net-
13 works and the vulnerability of such networks and mobile
14 devices to cyberattacks and surveillance conducted by ad-
15 versaries.

16 (b) MATTERS TO BE INCLUDED.—The report re-
17 quired by subsection (a) shall include the following:

18 (1) An assessment of the degree to which pro-
19 viders of mobile service have addressed, are address-
20 ing, or have not addressed cybersecurity
21 vulnerabilities (including vulnerabilities the exploi-
22 tation of which could lead to surveillance conducted
23 by adversaries) identified by academic and inde-
24 pendent researchers, multistakeholder standards and
25 technical organizations, industry experts, and Fed-
26 eral agencies, including in relevant reports of—

1 (A) the National Telecommunications and
2 Information Administration;

3 (B) the National Institute of Standards
4 and Technology; and

5 (C) the Department of Homeland Security,
6 including—

7 (i) the Cybersecurity and Infrastruc-
8 ture Security Agency; and

9 (ii) the Science and Technology Direc-
10 torate.

11 (2) A discussion of—

12 (A) the degree to which customers (includ-
13 ing consumers, companies, and government
14 agencies) consider cybersecurity as a factor
15 when considering the purchase of mobile service
16 and mobile devices; and

17 (B) the commercial availability of tools,
18 frameworks, best practices, and other resources
19 for enabling such customers to evaluate cyber-
20 security risk and price tradeoffs.

21 (3) A discussion of the degree to which pro-
22 viders of mobile service have implemented cybersecu-
23 rity best practices and risk assessment frameworks.

24 (4) An estimate and discussion of the preva-
25 lence and efficacy of encryption and authentication

1 algorithms and techniques used in each of the fol-
2 lowing:

3 (A) Mobile service.

4 (B) Mobile communications equipment or
5 services.

6 (C) Commonly used mobile phones and
7 other mobile devices.

8 (D) Commonly used mobile operating sys-
9 tems and communications software and applica-
10 tions.

11 (5) A discussion of the barriers for providers of
12 mobile service to adopt more efficacious encryption
13 and authentication algorithms and techniques and to
14 prohibit the use of older encryption and authentica-
15 tion algorithms and techniques with established
16 vulnerabilities in mobile service, mobile communica-
17 tions equipment or services, and mobile phones and
18 other mobile devices.

19 (6) An estimate and discussion of the preva-
20 lence, usage, and availability of technologies that au-
21 thenticate legitimate mobile service and mobile com-
22 munications equipment or services to which mobile
23 phones and other mobile devices are connected.

24 (7) An estimate and discussion of the preva-
25 lence, costs, commercial availability, and usage by

1 adversaries in the United States of cell site simula-
2 tors (often known as international mobile subscriber
3 identity-catchers) and other mobile service surveil-
4 lance and interception technologies.

5 (c) CONSULTATION.—In preparing the report re-
6 quired by subsection (a), the Assistant Secretary shall, to
7 the degree practicable, consult with—

8 (1) the Federal Communications Commission;

9 (2) the National Institute of Standards and
10 Technology;

11 (3) the intelligence community;

12 (4) the Cybersecurity and Infrastructure Secu-
13 rity Agency of the Department of Homeland Secu-
14 rity;

15 (5) the Science and Technology Directorate of
16 the Department of Homeland Security;

17 (6) academic and independent researchers with
18 expertise in privacy, encryption, cybersecurity, and
19 network threats;

20 (7) participants in multistakeholder standards
21 and technical organizations (including the 3rd Gen-
22 eration Partnership Project and the Internet Engi-
23 neering Task Force);

24 (8) international stakeholders, in coordination
25 with the Department of State as appropriate;

1 (9) providers of mobile service, including small
2 providers (or the representatives of such providers)
3 and rural providers (or the representatives of such
4 providers);

5 (10) manufacturers, operators, and providers of
6 mobile communications equipment or services and
7 mobile phones and other mobile devices;

8 (11) developers of mobile operating systems and
9 communications software and applications; and

10 (12) other experts that the Assistant Secretary
11 considers appropriate.

12 (d) SCOPE OF REPORT.—The Assistant Secretary
13 shall—

14 (1) limit the report required by subsection (a)
15 to mobile service networks;

16 (2) exclude consideration of 5G protocols and
17 networks in the report required by subsection (a);

18 (3) limit the assessment required by subsection
19 (b)(1) to vulnerabilities that have been shown to
20 be—

21 (A) exploited in non-laboratory settings; or

22 (B) feasibly and practicably exploitable in
23 real-world conditions; and

24 (4) consider in the report required by sub-
25 section (a) vulnerabilities that have been effectively

1 mitigated by manufacturers of mobile phones and
2 other mobile devices.

3 (e) FORM OF REPORT.—

4 (1) CLASSIFIED INFORMATION.—The report re-
5 quired by subsection (a) shall be produced in unclas-
6 sified form but may contain a classified annex.

7 (2) POTENTIALLY EXPLOITABLE UNCLASSIFIED
8 INFORMATION.—The Assistant Secretary shall re-
9 duct potentially exploitable unclassified information
10 from the report required by subsection (a) but shall
11 provide an unredacted form of the report to the
12 committees described in such subsection.

13 (f) AUTHORIZATION OF APPROPRIATIONS.—There is
14 authorized to be appropriated to carry out this section
15 \$500,000 for fiscal year 2022. Such amount is authorized
16 to remain available through fiscal year 2023.

17 (g) DEFINITIONS.—In this section:

18 (1) ADVERSARY.—The term “adversary” in-
19 cludes—

20 (A) any unauthorized hacker or other in-
21 truder into a mobile service network; and

22 (B) any foreign government or foreign
23 nongovernment person engaged in a long-term
24 pattern or serious instances of conduct signifi-
25 cantly adverse to the national security of the

1 United States or security and safety of United
2 States persons.

3 (2) ASSISTANT SECRETARY.—The term “Assist-
4 ant Secretary” means the Assistant Secretary of
5 Commerce for Communications and Information.

6 (3) ENTITY.—The term “entity” means a part-
7 nership, association, trust, joint venture, corpora-
8 tion, group, subgroup, or other organization.

9 (4) INTELLIGENCE COMMUNITY.—The term
10 “intelligence community” has the meaning given
11 that term in section 3 of the National Security Act
12 of 1947 (50 U.S.C. 3003).

13 (5) MOBILE COMMUNICATIONS EQUIPMENT OR
14 SERVICE.—The term “mobile communications equip-
15 ment or service” means any equipment or service
16 that is essential to the provision of mobile service.

17 (6) MOBILE SERVICE.—The term “mobile serv-
18 ice” means, to the extent provided to United States
19 customers, either or both of the following services:

20 (A) Commercial mobile service (as defined
21 in section 332(d) of the Communications Act of
22 1934 (47 U.S.C. 332(d))).

23 (B) Commercial mobile data service (as de-
24 fined in section 6001 of the Middle Class Tax

3 (7) PERSON.—The term “person” means an in-
4 dividual or entity.

5 (8) UNITED STATES PERSON.—The term
6 “United States person” means—

7 (A) an individual who is a United States
8 citizen or an alien lawfully admitted for perma-
9 nent residence to the United States;

(B) an entity organized under the laws of the United States or any jurisdiction within the United States, including a foreign branch of such an entity; or

14 (C) any person in the United States.

Passed the House of Representatives December 1,
2021.

Attest: CHERYL L. JOHNSON,
Clerk.