

118TH CONGRESS
1ST SESSION

H. R. 1123

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.

IN THE HOUSE OF REPRESENTATIVES

FEBRUARY 21, 2023

Ms. ESHOO (for herself and Mrs. CAMMACK) introduced the following bill;
which was referred to the Committee on Energy and Commerce

A BILL

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,*

3 **SECTION 1. SHORT TITLE.**

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

1 **SEC. 2. REPORT ON CYBERSECURITY OF MOBILE SERVICE**
2 **NETWORKS.**

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

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

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

24 (A) the National Telecommunications and
25 Information Administration;

1 (B) the National Institute of Standards
2 and Technology; and

3 (C) the Department of Homeland Security,
4 including—

5 (i) the Cybersecurity and Infrastruc-
6 ture Security Agency; and

7 (ii) the Science and Technology Direc-
8 torate.

9 (2) A discussion of—

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

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

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

22 (4) An estimate and discussion of the preva-
23 lence and efficacy of encryption and authentication
24 algorithms and techniques used in each of the fol-
25 lowing:

1 (A) Mobile service.

2 (B) Mobile communications equipment or
3 services.

4 (C) Commonly used mobile phones and
5 other mobile devices.

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

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

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

22 (7) An estimate and discussion of the preva-
23 lence, costs, commercial availability, and usage by
24 adversaries in the United States of cell site simula-
25 tors (often known as international mobile subscriber

1 identity catchers) and other mobile service surveil-
2 lance and interception technologies.

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

6 (1) the Federal Communications Commission;

7 (2) the National Institute of Standards and
8 Technology;

9 (3) the intelligence community;

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

13 (5) the Science and Technology Directorate of
14 the Department of Homeland Security;

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

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

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

24 (9) providers of mobile service, including small
25 providers (or the representatives of such providers)

1 and rural providers (or the representatives of such
2 providers);

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

6 (11) developers of mobile operating systems and
7 communications software and applications; and

8 (12) other experts that the Assistant Secretary
9 considers appropriate.

10 (d) SCOPE OF REPORT.—The Assistant Secretary
11 shall—

12 (1) limit the report required by subsection (a)
13 to mobile service networks;

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

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

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

20 (B) feasibly and practicably exploitable in
21 real-world conditions; and

22 (4) consider in the report required by sub-
23 section (a) vulnerabilities that have been effectively
24 mitigated by manufacturers of mobile phones and
25 other mobile devices.

1 (e) FORM OF REPORT.—

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

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

11 (f) AUTHORIZATION OF APPROPRIATIONS.—There is
12 authorized to be appropriated to carry out this section
13 \$500,000 for fiscal year 2024. Such amount is authorized
14 to remain available through fiscal year 2025.

15 (g) DEFINITIONS.—In this section:

16 (1) ADVERSARY.—The term “adversary” in-
17 cludes—

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

20 (B) any foreign government or foreign
21 nongovernment person engaged in a long-term
22 pattern or serious instances of conduct signifi-
23 cantly adverse to the national security of the
24 United States or security and safety of United
25 States persons.

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

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

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

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

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

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

21 (B) Commercial mobile data service (as de-
22 fined in section 6001 of the Middle Class Tax
23 Relief and Job Creation Act of 2012 (47 U.S.C.
24 1401)).

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

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

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

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

12 (C) any person in the United States.

○