

117TH CONGRESS  
1ST SESSION

# H. R. 2685

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

APRIL 20, 2021

Ms. ESHOO (for herself and Mr. KINZINGER) 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 Congress a report examining the cy-  
7 bersecurity of mobile service networks and the vulner-  
8 ability of such networks and mobile devices to cyberattacks  
9 and surveillance conducted by adversaries.

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

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

21 (A) the National Telecommunications and  
22 Information Administration;

23 (B) the National Institute of Standards  
24 and Technology; and

25 (C) the Department of Homeland Security,  
26 including—

1 (i) the Cybersecurity and Infrastruc-  
2 ture Security Agency; and

3 (ii) the Science and Technology Direc-  
4 torate.

5 (2) A discussion of—

6 (A) the degree to which customers (includ-  
7 ing consumers, companies, and government  
8 agencies) consider cybersecurity as a factor  
9 when considering the purchase of mobile serv-  
10 ice; and

11 (B) the commercial availability of tools,  
12 frameworks, best practices, and other resources  
13 for enabling such customers to evaluate risk  
14 and price tradeoffs.

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

18 (4) An estimate and discussion of the preva-  
19 lence and efficacy of encryption and authentication  
20 algorithms and techniques used in each of the fol-  
21 lowing:

22 (A) Mobile service.

23 (B) Mobile communications equipment or  
24 services.

1 (C) Commonly used mobile phones and  
2 other mobile devices.

3 (D) Commonly used mobile operating sys-  
4 tems and communications software and applica-  
5 tions.

6 (5) Barriers for providers of mobile service to  
7 adopt more efficacious encryption and authentication  
8 algorithms and techniques and to prohibit the use of  
9 older encryption and authentication algorithms and  
10 techniques with established vulnerabilities in mobile  
11 service, mobile communications equipment or serv-  
12 ices, and mobile phones and other mobile devices.

13 (6) The prevalence, usage, and availability of  
14 technologies that authenticate legitimate mobile  
15 service and mobile communications equipment or  
16 services to which mobile phones and other mobile de-  
17 vices are connected.

18 (7) The prevalence, costs, commercial avail-  
19 ability, and usage by adversaries in the United  
20 States of cell site simulators (often known as inter-  
21 national mobile subscriber identity-catchers) and  
22 other mobile service surveillance and interception  
23 technologies.

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

4               (1) the Commission;

5               (2) the National Institute of Standards and  
6       Technology;

7               (3) the intelligence community;

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

11              (5) the Science and Technology Directorate of  
12      the Department of Homeland Security;

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

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

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

22              (9) providers of mobile service;

23              (10) manufacturers, operators, and providers of  
24      mobile communications equipment or services and  
25      mobile phones and other mobile devices;

1           (11) developers of mobile operating systems and  
2       communications software and applications; and

3           (12) other experts that the Assistant Secretary  
4       considers appropriate.

5       (d) SCOPE OF REPORT.—The Assistant Secretary  
6       shall—

7           (1) limit the report required by subsection (a)  
8       to mobile service networks;

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

11          (3) limit the assessment required by subsection  
12      (b)(1) to vulnerabilities that have been shown to  
13      be—

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

15                  (B) feasibly and practicably exploitable in  
16      real-world conditions; and

17          (4) consider in the report required by sub-  
18      section (a) vulnerabilities that have been effectively  
19      mitigated by manufacturers of mobile phones and  
20      other mobile devices.

21       (e) FORM OF REPORT.—The report required by sub-  
22      section (a) shall be produced in unclassified form but may  
23      contain a classified annex.

24       (f) AUTHORIZATION OF APPROPRIATIONS.—There is  
25      authorized to be appropriated to carry out this section

1 \$500,000 for fiscal year 2021. Such amount is authorized  
2 to remain available through fiscal year 2022.

3 (g) DEFINITIONS.—In this section:

4 (1) ADVERSARY.—The term “adversary” in-  
5 cludes—

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

8 (B) any foreign government or foreign  
9 nongovernment person engaged in a long-term  
10 pattern or serious instances of conduct signifi-  
11 cantly adverse to the national security of the  
12 United States or security and safety of United  
13 States persons.

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

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

20 (4) INTELLIGENCE COMMUNITY.—The term  
21 “intelligence community” has the meaning given  
22 that term in section 3 of the National Security Act  
23 of 1947 (50 U.S.C. 3003).

24 (5) MOBILE COMMUNICATIONS EQUIPMENT OR  
25 SERVICE.—The term “mobile communications equip-

1       ment or service” means any equipment or service  
2       that is essential to the provision of mobile service.

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

6               (A) Commercial mobile service (as defined  
7       in section 332(d) of the Communications Act of  
8       1934 (47 U.S.C. 332(d))).

9               (B) Commercial mobile data service (as de-  
10       fined in section 6001 of the Middle Class Tax  
11       Relief and Job Creation Act of 2012 (47 U.S.C.  
12       1401)).

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

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

17              (A) an individual who is a United States  
18       citizen or an alien lawfully admitted for perma-  
19       nent residence to the United States;

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

24              (C) any person in the United States.

○