

**AMENDMENT TO SUBTITLE K**  
**OFFERED BY M**\_\_ . \_\_\_\_\_

In section 31102, strike “In addition” and insert  
“(a) APPROPRIATION.—In addition”.

Add at the end of section 31102 the following:

1 (b) REPORT ON CYBERSECURITY OF MOBILE SERV-  
2 ICE NETWORKS.—

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

14 (2) MATTERS TO BE INCLUDED.—The report  
15 required by paragraph (1) shall include the fol-  
16 lowing:

1 (A) An assessment of the degree to which  
2 providers of mobile service have addressed, are  
3 addressing, or have not addressed cybersecurity  
4 vulnerabilities (including vulnerabilities the ex-  
5 ploitation of which could lead to surveillance  
6 conducted by adversaries) identified by aca-  
7 demic and independent researchers, multistake-  
8 holder standards and technical organizations,  
9 industry experts, and Federal agencies, includ-  
10 ing in relevant reports of—

11 (i) the National Telecommunications  
12 and Information Administration;

13 (ii) the National Institute of Stand-  
14 ards and Technology; and

15 (iii) the Department of Homeland Se-  
16 curity, including—

17 (I) the Cybersecurity and Infra-  
18 structure Security Agency; and

19 (II) the Science and Technology  
20 Directorate.

21 (B) A discussion of—

22 (i) the degree to which customers (in-  
23 cluding consumers, companies, and govern-  
24 ment agencies) consider cybersecurity as a

1 factor when considering the purchase of  
2 mobile service and mobile devices; and

3 (ii) the commercial availability of  
4 tools, frameworks, best practices, and  
5 other resources for enabling such cus-  
6 tomers to evaluate risk and price tradeoffs.

7 (C) A discussion of the degree to which  
8 providers of mobile service have implemented  
9 cybersecurity best practices and risk assessment  
10 frameworks.

11 (D) An estimate and discussion of the  
12 prevalence and efficacy of encryption and au-  
13 thentication algorithms and techniques used in  
14 each of the following:

15 (i) Mobile service.

16 (ii) Mobile communications equipment  
17 or services.

18 (iii) Commonly used mobile phones  
19 and other mobile devices.

20 (iv) Commonly used mobile operating  
21 systems and communications software and  
22 applications.

23 (E) Barriers for providers of mobile service  
24 to adopt more efficacious encryption and au-  
25 thentication algorithms and techniques and to

1 prohibit the use of older encryption and authen-  
2 tication algorithms and techniques with estab-  
3 lished vulnerabilities in mobile service, mobile  
4 communications equipment or services, and mo-  
5 bile phones and other mobile devices.

6 (F) The prevalence, usage, and availability  
7 of technologies that authenticate legitimate mo-  
8 bile service and mobile communications equip-  
9 ment or services to which mobile phones and  
10 other mobile devices are connected.

11 (G) The prevalence, costs, commercial  
12 availability, and usage by adversaries in the  
13 United States of cell site simulators (often  
14 known as international mobile subscriber iden-  
15 tity-catchers) and other mobile service surveil-  
16 lance and interception technologies.

17 (3) CONSULTATION.—In preparing the report  
18 required by paragraph (1), the Assistant Secretary  
19 shall, to the degree practicable, consult with—

20 (A) the Federal Communications Commis-  
21 sion;

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

24 (C) the intelligence community;

1 (D) the Cybersecurity and Infrastructure  
2 Security Agency of the Department of Home-  
3 land Security;

4 (E) the Science and Technology Direc-  
5 torate of the Department of Homeland Secu-  
6 rity;

7 (F) academic and independent researchers  
8 with expertise in privacy, encryption, cybersecu-  
9 rity, and network threats;

10 (G) participants in multistakeholder stand-  
11 ards and technical organizations (including the  
12 3rd Generation Partnership Project and the  
13 Internet Engineering Task Force);

14 (H) international stakeholders, in coordi-  
15 nation with the Department of State as appro-  
16 priate;

17 (I) providers of mobile service, including  
18 small providers (or the representatives of such  
19 providers) and rural providers (or the rep-  
20 resentatives of such providers);

21 (J) manufacturers, operators, and pro-  
22 viders of mobile communications equipment or  
23 services and mobile phones and other mobile de-  
24 vices;

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

4 (L) other experts that the Assistant Sec-  
5 retary considers appropriate.

6 (4) SCOPE OF REPORT.—The Assistant Sec-  
7 retary shall—

8 (A) limit the report required by paragraph  
9 (1) to mobile service networks;

10 (B) exclude consideration of 5G protocols  
11 and networks in the report required by para-  
12 graph (1);

13 (C) limit the assessment required by para-  
14 graph (2)(A) to vulnerabilities that have been  
15 shown to be—

16 (i) exploited in non-laboratory set-  
17 tings; or

18 (ii) feasibly and practicably exploitable  
19 in real-world conditions; and

20 (D) consider in the report required by  
21 paragraph (1) vulnerabilities that have been ef-  
22 fectively mitigated by manufacturers of mobile  
23 phones and other mobile devices.

24 (5) FORM OF REPORT.—

1 (A) CLASSIFIED INFORMATION.—The re-  
2 port required by paragraph (1) shall be pro-  
3 duced in unclassified form but may contain a  
4 classified annex.

5 (B) POTENTIALLY EXPLOITABLE UNCLAS-  
6 SIFIED INFORMATION.—The Assistant Sec-  
7 retary shall redact potentially exploitable un-  
8 classified information from the report required  
9 by paragraph (1) but shall provide an  
10 unredacted form of the report to the commit-  
11 tees described in such subsection.

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

17 (7) DEFINITIONS.—In this section:

18 (A) ADVERSARY.—The term “adversary”  
19 includes—

20 (i) any unauthorized hacker or other  
21 intruder into a mobile service network; and

22 (ii) any foreign government or foreign  
23 nongovernment person engaged in a long-  
24 term pattern or serious instances of con-  
25 duct significantly adverse to the national

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

3 (B) ASSISTANT SECRETARY.—The term  
4 “Assistant Secretary” means the Assistant Sec-  
5 retary of Commerce for Communications and  
6 Information.

7 (C) ENTITY.—The term “entity” means a  
8 partnership, association, trust, joint venture,  
9 corporation, group, subgroup, or other organi-  
10 zation.

11 (D) INTELLIGENCE COMMUNITY.—The  
12 term “intelligence community” has the meaning  
13 given that term in section 3 of the National Se-  
14 curity Act of 1947 (50 U.S.C. 3003).

15 (E) MOBILE COMMUNICATIONS EQUIP-  
16 MENT OR SERVICE.—The term “mobile commu-  
17 nications equipment or service” means any  
18 equipment or service that is essential to the  
19 provision of mobile service.

20 (F) MOBILE SERVICE.—The term “mobile  
21 service” means, to the extent provided to  
22 United States customers, either or both of the  
23 following services:



1 (i) Commercial mobile service (as de-  
2 fined in section 332(d) of the Communica-  
3 tions Act of 1934 (47 U.S.C. 332(d))).

4 (ii) Commercial mobile data service  
5 (as defined in section 6001 of the Middle  
6 Class Tax Relief and Job Creation Act of  
7 2012 (47 U.S.C. 1401)).

8 (G) PERSON.—The term “person” means  
9 an individual or entity.

10 (H) UNITED STATES PERSON.—The term  
11 “United States person” means—

12 (i) an individual who is a United  
13 States citizen or an alien lawfully admitted  
14 for permanent residence to the United  
15 States;

16 (ii) an entity organized under the laws  
17 of the United States or any jurisdiction  
18 within the United States, including a for-  
19 eign branch of such an entity; or

20 (iii) any person in the United States.

