117TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPORT
117–186

UNDERSTANDING CYBERSECURITY OF MOBILE NETWORKS ACT

NOVEMBER 30, 2021.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. PALLONE, from the Committee on Energy and Commerce, submitted the following

R E P O R T

[To accompany H.R. 2685]

The Committee on Energy and Commerce, to whom was referred the bill (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, having considered the same, reports favorably thereon with an amendment and recommends that the bill as amended do pass.

CONTENTS

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Understanding Cybersecurity of Mobile Networks Act".

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

(a) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, the Assistant Secretary, in consultation with the Department of Homeland Security, shall submit to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report examining the cybersecurity of mobile service networks and the vulnerability of such networks and mobile devices to cyberattacks and surveillance conducted by adversaries.

(b) MATTERS TO BE INCLUDED.—The report required by subsection (a) shall include the following:

(1) An assessment of the degree to which providers of mobile service have addressed, are addressing, or have not addressed cybersecurity vulnerabilities (including vulnerabilities the exploitation of which could lead to surveillance conducted by adversaries) identified by academic and independent researchers, multistakeholder standards and technical organizations, industry experts, and Federal agencies, including in relevant reports of—

(A) the National Telecommunications and Information Administration;

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

(C) the Department of Homeland Security, including—

(i) the Cybersecurity and Infrastructure Security Agency; and

(ii) the Science and Technology Directorate.

(2) A discussion of—

(A) the degree to which customers (including consumers, companies, and government agencies) consider cybersecurity as a factor when considering the purchase of mobile service and mobile devices; and

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

(3) A discussion of the degree to which providers of mobile service have implemented cybersecurity best practices and risk assessment frameworks.

(4) An estimate and discussion of the prevalence and efficacy of encryption and authentication algorithms and techniques used in each of the following:

(A) Mobile service.

(B) Mobile communications equipment or services.

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

(D) Commonly used mobile operating systems and communications software and applications.

(5) Barriers for providers of mobile service to adopt more efficacious encryption and authentication algorithms and techniques and to prohibit the use of older encryption and authentication algorithms and techniques with established vulnerabilities in mobile service, mobile communications equipment or services, and mobile phones and other mobile devices.

(6) The prevalence, usage, and availability of technologies that authenticate legitimate mobile service and mobile communications equipment or services to which mobile phones and other mobile devices are connected.

(7) The prevalence, costs, commercial availability, and usage by adversaries in the United States of cell site simulators (often known as international mobile subscriber identity-catchers) and other mobile service surveillance and interception technologies.

(c) CONSULTATION.—In preparing the report required by subsection (a), the Assistant Secretary shall, to the degree practicable, consult with—

(1) the Federal Communications Commission;

(2) the National Institute of Standards and Technology;

(3) the intelligence community;

(4) the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security;

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

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

(7) participants in multistakeholder standards and technical organizations (including the 3rd Generation Partnership Project and the Internet Engineering Task Force);

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

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

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

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

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

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

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

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

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

(A) exploited in non-laboratory settings; or

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

(4) consider in the report required by subsection (a) vulnerabilities that have been effectively mitigated by manufacturers of mobile phones and other mobile devices.

(e) FORM OF REPORT.—

(1) CLASSIFIED INFORMATION.—The report required by subsection (a) shall be produced in unclassified form but may contain a classified annex.

(2) POTENTIALLY EXPLOITABLE UNCLASSIFIED INFORMATION.—The Assistant Secretary shall redact potentially exploitable unclassified information from the report required by subsection (a) but shall provide an unredacted form of the report to the committees described in such subsection.

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

(g) DEFINITIONS.—In this section:

(1) ADVERSARY.—The term "adversary" includes—

(A) any unauthorized hacker or other intruder into a mobile service network; and

(B) any foreign government or foreign nongovernment person engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons.

(2) ASSISTANT SECRETARY.—The term "Assistant Secretary" means the Assistant Secretary of Commerce for Communications and Information.

(3) ENTITY.—The term "entity" means a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization.

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

(5) MOBILE COMMUNICATIONS EQUIPMENT OR SERVICE.—The term "mobile communications equipment or service" means any equipment or service that is essential to the provision of mobile service.

(6) MOBILE SERVICE.—The term "mobile service" means, to the extent provided to United States customers, either or both of the following services:

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

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

(7) PERSON.—The term "person" means an individual or entity.

(8) UNITED STATES PERSON.—The term "United States person" means—

(A) an individual who is a United States citizen or an alien lawfully admitted for permanent 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

(C) any person in the United States.

I. PURPOSE AND SUMMARY

H.R. 2685, the "Understanding Cybersecurity of Mobile Networks Act," would require the National Telecommunications and Information Administration (NTIA) to examine and report on the cybersecurity of mobile service networks (excluding 5G) and mobile de-

vices. The report shall discuss, among other things, the degree to which mobile services providers have addressed vulnerabilities; cybersecurity best practices and risk assessment frameworks; and the prevalence and usage of cell site simulators and other surveillance technologies used by adversaries.

II. BACKGROUND AND NEED FOR LEGISLATION

Federal agencies, academic researchers, and independent experts have examined various and disparate aspects of, specific threats to, and vulnerabilities of the cybersecurity of mobile devices and networks.[1] Providers of mobile services, along with manufacturers of mobile devices and other companies, have responded to many vulnerabilities and threats.[2] However, recent cybersecurity developments show that vulnerabilities continue to exist in mobile cybersecurity, including threats of mobile data interception by cell site simulators,[3] identity theft via fraudulent SIM swaps,[4] and surveillance enabled by spyware installed on mobile devices.[5] Policymakers lack a holistic accounting of what vulnerabilities have been addressed or are being addressed and which ones persist.

While policymakers and industry actors are appropriately focused on cybersecurity of 5G networks, cybersecurity related to 2G, 3G, and 4G networks is of particular public policy interest because these networks host a vast majority of Americans' mobile calls and text messages and mobile internet data traffic.

While many Federal agencies have authorities and responsibilities related to cybersecurity, Congress has tasked NTIA to foster safety and national security of telecommunications networks.[6]

III. COMMITTEE HEARINGS

For the purposes of clause 3(c) of rule XIII of the Rules of the House of Representatives, the following hearings were used to develop or consider H.R. 2685:

The Subcommittee on Communications and Technology held a hearing on April 21, 2021, entitled "Leading the Wireless Future: Securing American Network Technology." The Subcommittee received testimony from the following witnesses:

- John Baker, Senior Vice President, Business Development, Mavenir;
- John Mezzalingua, Chief Executive Officer, JMA Wireless;
- Tim Donovan, SVP, Legislative Affairs, Competitive Carriers Association;
- Tareq Amin, EVP and Group Chief Technology Officer, Rakuten Mobile; and
- Diane Rinaldo, Executive Director, Open RAN Policy Coalition.

The Subcommittee on Communications and Technology held a legislative hearing on June 30, 2021, entitled "A Safe Wireless Future: Securing our Networks and Supply Chains." The Subcommittee received testimony from the following witnesses:

---

[1] *See, e.g.*, Department of Homeland Security, *Study on Mobile Device Security* (April 2017).
[2] *See, e.g.*, CTIA, *SS7 and FCC CSRIC Recommendations* (2017).
[3] Lily Hay Newman, *One Small Fix Would Curb Stingray Surveillance*, Wired (Jan. 27, 2020).
[4] M.J. Kelly, *Mozilla Explains: SIM swapping*, Mozilla (Apr. 7, 2021).
[5] Mitchell Clark, *NSO's Pegasus spyware: here's what we know*, The Verge (July 23, 2021).
[6] National Telecommunications and Information Administration Organization Act § 102(c)(2), 47 U.S.C. § 901(c)(2).

• Dileep Srihari, Senior Policy Counsel, Access Partnership;
• Dean Brenner, SVP, Spectrum Strategy & Tech Policy, Qualcomm Incorporated;
• Jason Boswell, Head of Security, Network Product Solutions, N.A., Ericsson; and
• Clete Johnson, Senior Fellow, Strategic Technologies Program, Center for Strategic and International Studies.

IV. COMMITTEE CONSIDERATION

Representatives Anna G. Eshoo (D–CA) and Adam Kinzinger (R–IL) introduced H.R. 2685, the "Understanding Cybersecurity of Mobile Networks Act," on April 20, 2021, which was referred to the Committee on Energy and Commerce. Subsequently, on April 21, 2021, H.R. 2685 was referred to the Subcommittee on Communications and Technology. A legislative hearing was held on the bill on June 30, 2021.

On July 20, 2021, the Subcommittee on Communications and Technology was discharged from further consideration of the bill. On July 21, 2021, the full Committee met in open markup session, pursuant to notice, to consider H.R. 2685 and 23 other bills. During consideration of the bill, an amendment in the nature of a substitute (AINS) offered by Representative Eshoo was agreed to by a voice vote. Upon conclusion of consideration of the bill, the full Committee agreed to a motion on final passage offered by Representative Pallone (D–NJ), Chairman of the Committee, to order H.R. 2685 reported favorably to the House, amended, by a voice vote.

V. COMMITTEE VOTES

Clause 3(b) of rule XIII of the Rules of the House of Representatives requires the Committee to list each record vote on the motion to report legislation and amendments thereto. The Committee advises that there were no record votes taken on H.R. 2685, including a motion by Mr. Pallone ordering H.R. 2685 favorably reported to the House, amended.

VI. OVERSIGHT FINDINGS

Pursuant to clause 3(c)(1) of rule XIII and clause 2(b)(1) of rule X of the Rules of the House of Representatives, the oversight findings and recommendations of the Committee are reflected in the descriptive portion of the report.

VII. NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

Pursuant to 3(c)(2) of rule XIII of the Rules of the House of Representatives, the Committee adopts as its own the estimate of new budget authority, entitlement authority, or tax expenditures or revenues contained in the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

The Committee has requested but not received from the Director of the Congressional Budget Office a statement as to whether this bill contains any new budget authority, spending authority, credit

authority, or an increase or decrease in revenues or tax expenditures.

VIII. FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

IX. STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of rule XIII, the general performance goal or objective of this legislation is to examine and report on cybersecurity of mobile service networks and the vulnerabilities of such networks to cyberattacks and surveillance conducted by adversaries.

X. DUPLICATION OF FEDERAL PROGRAMS

Pursuant to clause 3(c)(5) of rule XIII, no provision of H.R. 2685 is known to be duplicative of another Federal program, including any program that was included in a report to Congress pursuant to section 21 of Public Law 111–139 or the most recent Catalog of Federal Domestic Assistance.

XI. COMMITTEE COST ESTIMATE

Pursuant to clause 3(d)(1) of rule XIII, the Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

XII. EARMARKS, LIMITED TAX BENEFITS, AND LIMITED TARIFF BENEFITS

Pursuant to clause 9(e), 9(f), and 9(g) of rule XXI, the Committee finds that H.R. 2685 contains no earmarks, limited tax benefits, or limited tariff benefits.

XIII. ADVISORY COMMITTEE STATEMENT

No advisory committee within the meaning of section 5(b) of the Federal Advisory Committee Act was created by this legislation.

XIV. APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

XV. SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short title

Section 1 designates that the short title may be cited as the "Understanding Cybersecurity of Mobile Networks Act."

Sec. 2. Report on cybersecurity of mobile service networks

Subsection (a) directs the Assistant Secretary of Commerce for Communications and Information (i.e., the Director of the National Telecommunications and Information Administration), in consulta-

tion with the Department of Homeland Security, to submit to Congress, not later than one year after enactment, a report examining the cybersecurity of mobile service networks and the vulnerability of such networks and mobile devices to cyberattacks and surveillance conducted by adversaries.

Subsection (b) requires the report to include (1) an assessment of the degree to which providers of mobile service have addressed cybersecurity vulnerabilities; (2) a discussion of the degree to which customers consider cybersecurity; (3) a discussion of best practices and risk assessment frameworks; (4) an estimate and discussion of aspects of encryption and authentication algorithms and techniques; (5) a discussion of barriers to more efficacious encryption; (6) an estimate and discussion of aspects of authentication; and (7) an estimate and discussion of aspects of cell site simulators and other surveillance technologies.

Subsection (c) requires the Assistant Secretary, in preparing the report, to consult certain Federal agencies; researchers; participants in multistakeholder standards organizations; international stakeholders; industry representatives; and other experts.

Subsection (d) provides certain limitations on the scope of the report, including that the report shall exclude consideration of 5G and limit vulnerabilities to those that have been exploited or are feasibly exploitable.

Subsection (e) provides that the report shall be produced in an unclassified form, shall redact potentially exploitable unclassified information, and may contain a classified annex.

Subsection (f) authorizes to be appropriated $500,000 to carry out this section.

Subsection (g) provides definitions for certain terms used in the Act, including adversary, mobile communications equipment or service, and mobile service.

XVI. CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

There are no changes to existing law made by the bill H.R. 2685.

○