AMENDMENT IN THE NATURE OF A SUBSTITUTE TO H.R. 2685

OFFERED BY Ms. Eshoo

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 equip-

ment 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.

☒