

Committee Print

[SHOWING THE TEXT OF H.R. 2881 AS FORWARDED BY THE SUBCOMMITTEE
ON COMMUNICATIONS AND TECHNOLOGY ON NOVEMBER 14, 2019]

116TH CONGRESS
1ST SESSION

H. R. 2881

To require the President to develop a strategy to ensure the security of next generation mobile telecommunications systems and infrastructure in the United States and to assist allies and strategic partners in maximizing the security of next generation mobile telecommunications systems, infrastructure, and software, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

MAY 21, 2019

Ms. SPANBERGER (for herself, Ms. STEFANIK, Ms. SLOTKIN, Mr. ROONEY of Florida, Mr. O'HALLERAN, and Mrs. BROOKS of Indiana) introduced the following bill; which was referred to the Committee on Energy and Commerce, and in addition to the Committee on Foreign Affairs, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To require the President to develop a strategy to ensure the security of next generation mobile telecommunications systems and infrastructure in the United States and to assist allies and strategic partners in maximizing the security of next generation mobile telecommunications systems, infrastructure, and software, 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 “Secure 5G and Beyond
5 Act of 2019”.

6 **SEC. 2. STRATEGY TO ENSURE SECURITY OF NEXT GEN-**
7 **ERATION WIRELESS COMMUNICATIONS SYS-**
8 **TEMS AND INFRASTRUCTURE.**

9 (a) **APPROPRIATE COMMITTEES OF CONGRESS DE-**
10 **FINED.**—In this section, the term “appropriate commit-

11 tees of Congress” means—
12 (1) the Permanent Select Committee on Intel-

13 ligence, the Committee on Energy and Commerce,
14 the Committee on Foreign Affairs, the Committee
15 on Armed Services, and the Committee on Home-

16 land Security of the House of Representatives; and
17 (2) the Select Committee on Intelligence, the
18 Committee on Commerce, Science, and Transpor-

19 tation, the Committee on Foreign Relations, the
20 Committee on Armed Services, and the Committee
21 on Homeland Security and Governmental Affairs of
22 the Senate.
23 (b) **STRATEGY REQUIRED.**—Not later than 180 days
24 after the date of the enactment of this Act, the President,
25 in consultation with the Chairman of the Federal Commu-

1 nications Commission, the Assistant Secretary of Com-
2 merce for Communications and Information, the Secretary
3 of Homeland Security, the Director of National Intel-
4 ligence, the Attorney General, the Secretary of Defense,
5 and the Secretary of State, shall develop and submit to
6 the appropriate committees of Congress a strategy—

7 (1) to ensure the security of 5th and future
8 generations wireless communications systems and in-
9 frastructure within the United States;

10 (2) to provide technical assistance to mutual de-
11 fense treaty allies of the United States, strategic
12 partners of the United States, and other countries,
13 when in the security interests of the United States,
14 to maximize the security of 5th and future genera-
15 tions wireless communications systems and infra-
16 structure inside their countries; and

17 (3) to protect the competitiveness of United
18 States companies, privacy of United States con-
19 sumers, and integrity and impartiality of standards-
20 setting bodies related to 5th and future generations
21 wireless communications systems and infrastructure.

22 (c) DESIGNATION.—The strategy developed under
23 subsection (b) shall be known as the “Secure Next Genera-
24 tion Wireless Communications Strategy” (referred to in
25 this section as the “Strategy”).

1 (d) ELEMENTS.—The Strategy shall represent a
2 whole-of-government approach and shall include the fol-
3 lowing:

4 (1) A description of United States national and
5 economic security interests pertaining to the deploy-
6 ment of 5th and future generations wireless commu-
7 nications systems and infrastructure.

8 (2) An identification and assessment of poten-
9 tial security threats and vulnerabilities to the infra-
10 structure, equipment, systems, software, and vir-
11 tually defined networks that support 5th and future
12 generations wireless communications systems and in-
13 frastructure. The assessment shall include a com-
14 prehensive evaluation of the full range of threats to,
15 and unique security challenges posed by, 5th and fu-
16 ture generations wireless communications systems
17 and infrastructure, as well as steps that public and
18 private sector entities can take to mitigate such
19 threats.

20 (3) An identification and assessment of the
21 global competitiveness and vulnerabilities of United
22 States manufacturers and suppliers of 5th and fu-
23 ture generations wireless communications equip-
24 ment.

1 (4) A list of available domestic suppliers of 5th
2 and future generations wireless communications
3 equipment and other suppliers in countries that are
4 mutual defense allies or strategic partners of the
5 United States and a strategy to assess their ability
6 to produce and supply 5th generation and future
7 generations wireless communications systems and in-
8 frastructure.

9 (5) Identification of trusted supplier entities
10 from both inside and outside the United States that
11 are capable of producing and supplying to private in-
12 dustry infrastructure and systems equipment sup-
13 porting 5th and future generations wireless commu-
14 nications systems and infrastructure.

15 (6) Identification of where security gaps exist in
16 the United States domestic or mutual defense treaty
17 allies and strategic partners communications equip-
18 ment supply chain for 5th and future generations
19 wireless communications systems and infrastructure.

20 (7) Identification of incentives and policy op-
21 tions to help close or narrow any security gaps iden-
22 tified under paragraph (6) in, and ensure the eco-
23 nomic viability of, the United States domestic indus-
24 trial base, including research and development in
25 critical technologies and workforce development in

1 5th and future generations wireless communications
2 systems and infrastructure.

3 (8) Identification of incentives and policy op-
4 tions for leveraging the communications equipment
5 suppliers from mutual defense treaty allies, strategic
6 partners, and other countries to ensure that private
7 industry in the United States has adequate sources
8 for secure, effective, and reliable 5th and future gen-
9 erations wireless communications systems and infra-
10 structure equipment.

11 (9) A strategy for diplomatic engagement with
12 mutual defense treaty allies, strategic partners, and
13 other countries to share security risk information
14 and findings pertaining to 5th and future genera-
15 tions wireless communications systems and infra-
16 structure equipment and cooperation on mitigating
17 those risks.

18 (10) A strategy for engagement with private
19 sector communications infrastructure and systems
20 equipment developers to share information and find-
21 ings on 5th and future generations wireless commu-
22 nications systems and infrastructure equipment
23 standards to secure platforms.

24 (11) A strategy for engagement with private
25 sector communications infrastructure and systems

1 equipment developers to encourage the maximum
2 participation possible on standards-setting bodies re-
3 lated to such systems and infrastructure equipment
4 standards by public and private sector entities from
5 the United States.

6 (12) A strategy for diplomatic engagement with
7 mutual defense treaty allies, strategic partners, and
8 other countries to share information and findings on
9 5th and future generations wireless communications
10 systems and infrastructure equipment standards to
11 promote maximum interoperability, competitiveness,
12 openness, and secure platforms.

13 (13) A strategy for diplomatic engagement with
14 mutual defense treaty allies, strategic partners, and
15 other countries to share information and findings on
16 5th and future generations wireless communications
17 infrastructure and systems equipment concerning
18 the standards-setting bodies related to such systems
19 and infrastructure equipment to promote maximum
20 transparency, openness, impartiality, integrity and
21 neutrality.

22 (14) A strategy for joint testing environments
23 with mutual defense treaty allies, strategic partners,
24 and other countries to ensure a trusted marketplace

1 for 5th and future generations wireless communica-
2 tions systems and infrastructure equipment.

3 (15) A strategy for research and development
4 by the Federal Government, in close partnership
5 with trusted supplier entities, mutual defense treaty
6 allies, strategic partners, and other countries to
7 reach and maintain United States leadership in 5th
8 and future generations wireless communications sys-
9 tems and infrastructure security, including the de-
10 velopment of an ongoing monitoring capability of
11 5th and future generations wireless communications
12 systems to identify security vulnerabilities.

13 (16) Options for identifying and helping to
14 mitigate the security risks of 5th and future genera-
15 tions wireless communications systems and infra-
16 structure that have security flaws or vulnerabilities,
17 or are utilizing equipment sourced from countries of
18 concern, and that have already been put in place
19 within the systems and infrastructure of mutual de-
20 fense treaty allies, strategic partners, and other
21 countries, when in the security interests of the
22 United States.

23 (17) Development of a plan that includes a de-
24 scription of the roles and responsibilities of the ap-
25 propriate executive branch agencies and interagency

1 mechanisms for the Assistant Secretary of Com-
2 merce for Communications and Information to act
3 as the executive agent to coordinate implementation
4 of the Strategy, as provided in subsection (h).

5 (18) An identification of the key diplomatic, de-
6 velopment, intelligence, military, and economic re-
7 sources necessary to implement the Strategy, includ-
8 ing specific budgetary requests.

9 (19) A description of such legislative or admin-
10 istrative action as may be necessary to carry out the
11 Strategy.

12 (e) LIMITATION.—

13 (1) IN GENERAL.—The Strategy shall not in-
14 clude a recommendation or a proposal to nationalize
15 5th or future generations wireless communications
16 systems or infrastructure.

17 (2) FEDERAL AGENCY AUTHORITY.—Nothing in
18 this section shall be construed to limit the authority
19 or ability of a Federal agency to—

20 (A) conduct cybersecurity incident, threat,
21 or asset response and recovery activities;

22 (B) obtain or execute warrants or other in-
23 vestigative or intelligence tools; or

24 (C) provide assistance to a private entity
25 upon request of the entity.

1 (f) PUBLIC COMMENT.—Not later than 60 days after
2 the date of the enactment of this Act, the President shall
3 seek public comment regarding the development and im-
4 plementation of the Strategy.

5 (g) BRIEFING.—

6 (1) IN GENERAL.—Not later than 14 days after
7 the date on which the Strategy is completed, the As-
8 sistant Secretary of Commerce for Communications
9 and Information, and any other Federal officials
10 designated by the President, shall provide to the ap-
11 propriate committees of Congress a briefing on the
12 implementation of the Strategy.

13 (2) UNCLASSIFIED SETTING.—The briefing
14 under paragraph (1) shall be held in an unclassified
15 setting to the maximum extent possible.

16 (h) IMPLEMENTATION.—The Assistant Secretary of
17 Commerce for Communications and Information shall—

18 (1) act as the executive agent to coordinate im-
19 plementation of the Strategy;

20 (2) keep congressional committees apprised of
21 progress on implementation; and

22 (3) not implement any proposal or rec-
23 ommendation involving spectrum licensed by the
24 Commission unless the implementation of such pro-

1 posal or recommendation is first approved by the
2 Commission.

3 (i) FORM.—The Strategy shall be submitted to the
4 appropriate committees of Congress in unclassified form,
5 but may include a classified annex.

Amend the title so as to read: “A bill to require the President to develop a strategy to ensure the security of next generation wireless communications systems and infrastructure in the United States and to assist allies and strategic partners in maximizing the security of next generation wireless communications systems, infrastructure, and software, and for other purposes.”.