

**AMENDMENT IN THE NATURE OF A SUBSTITUTE
TO H.R. 2881**

OFFERED BY MR. O'HALLERAN OF ARIZONA AND MS. BROOKS OF INDIANA

Strike all after the enacting clause and insert the
following:

1 SECTION 1. SHORT TITLE.

2 This Act may be cited as the “Secure 5G and Beyond
3 Act of 2019”.

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

7 (a) APPROPRIATE COMMITTEES OF CONGRESS DE-
8 FINED.—In this section, the term “appropriate commit-
9 tees of Congress” means—

10 (1) the Permanent Select Committee on Intel-
11 ligence, the Committee on Energy and Commerce,
12 the Committee on Foreign Affairs, the Committee
13 on Armed Services, and the Committee on Home-
14 land Security of the House of Representatives; and

15 (2) the Select Committee on Intelligence, the
16 Committee on Commerce, Science, and Transpor-
17 tation, the Committee on Foreign Relations, the
18 Committee on Armed Services, and the Committee

1 on Homeland Security and Governmental Affairs of
2 the Senate.

3 (b) STRATEGY REQUIRED.—Not later than 180 days
4 after the date of the enactment of this Act, the President,
5 in consultation with the Chairman of the Federal Commu-
6 nications Commission, the Assistant Secretary of Com-
7 merce for Communications and Information, the Secretary
8 of Homeland Security, the Director of National Intel-
9 ligence, the Attorney General, the Secretary of Defense,
10 and the Secretary of State, shall develop and submit to
11 the appropriate committees of Congress a strategy—

12 (1) to ensure the security of 5th and future
13 generations wireless communications systems and in-
14 frastructure within the United States;

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

22 (3) to protect the competitiveness of United
23 States companies, privacy of United States con-
24 sumers, and integrity and impartiality of standards-

1 setting bodies related to 5th and future generations
2 wireless communications systems and infrastructure.

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

7 (d) ELEMENTS.—The Strategy shall represent a
8 whole-of-government approach and shall include the fol-
9 lowing:

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

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

1 (3) An identification and assessment of the
2 global competitiveness and vulnerabilities of United
3 States manufacturers and suppliers of 5th and fu-
4 ture generations wireless communications equip-
5 ment.

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

14 (5) Identification of trusted supplier entities
15 from both inside and outside the United States that
16 are capable of producing and supplying to private in-
17 dustry infrastructure and systems equipment sup-
18 porting 5th and future generations wireless commu-
19 nications systems and infrastructure.

20 (6) Identification of where security gaps exist in
21 the United States domestic or mutual defense treaty
22 allies and strategic partners communications equip-
23 ment supply chain for 5th and future generations
24 wireless communications systems and infrastructure.

1 (7) Identification of incentives and policy op-
2 tions to help close or narrow any security gaps iden-
3 tified under paragraph (6) in, and ensure the eco-
4 nomic viability of, the United States domestic indus-
5 trial base, including research and development in
6 critical technologies and workforce development in
7 5th and future generations wireless communications
8 systems and infrastructure.

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

17 (9) A strategy for diplomatic engagement with
18 mutual defense treaty allies, strategic partners, and
19 other countries to share security risk information
20 and findings pertaining to 5th and future genera-
21 tions wireless communications systems and infra-
22 structure equipment and cooperation on mitigating
23 those risks.

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

1 equipment developers to share information and find-
2 ings on 5th and future generations wireless commu-
3 nications systems and infrastructure equipment
4 standards to secure platforms.

5 (11) A strategy for engagement with private
6 sector communications infrastructure and systems
7 equipment developers to encourage the maximum
8 participation possible on standards-setting bodies re-
9 lated to such systems and infrastructure equipment
10 standards by public and private sector entities from
11 the United States.

12 (12) A strategy for diplomatic engagement with
13 mutual defense treaty allies, strategic partners, and
14 other countries to share information and findings on
15 5th and future generations wireless communications
16 systems and infrastructure equipment standards to
17 promote maximum interoperability, competitiveness,
18 openness, and secure platforms.

19 (13) A strategy for diplomatic engagement with
20 mutual defense treaty allies, strategic partners, and
21 other countries to share information and findings on
22 5th and future generations wireless communications
23 infrastructure and systems equipment concerning
24 the standards-setting bodies related to such systems
25 and infrastructure equipment to promote maximum

1 transparency, openness, impartiality, integrity and
2 neutrality.

3 (14) A strategy for joint testing environments
4 with mutual defense treaty allies, strategic partners,
5 and other countries to ensure a trusted marketplace
6 for 5th and future generations wireless communica-
7 tions systems and infrastructure equipment.

8 (15) A strategy for research and development
9 by the Federal Government, in close partnership
10 with trusted supplier entities, mutual defense treaty
11 allies, strategic partners, and other countries to
12 reach and maintain United States leadership in 5th
13 and future generations wireless communications sys-
14 tems and infrastructure security, including the de-
15 velopment of an ongoing monitoring capability of
16 5th and future generations wireless communications
17 systems to identify security vulnerabilities.

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

1 countries, when in the security interests of the
2 United States.

3 (17) Development of a plan that includes a de-
4 scription of the roles and responsibilities of the ap-
5 propriate executive branch agencies and interagency
6 mechanisms for the Assistant Secretary of Com-
7 merce for Communications and Information to act
8 as the executive agent to coordinate implementation
9 of the Strategy, as provided in subsection (h).

10 (18) An identification of the key diplomatic, de-
11 velopment, intelligence, military, and economic re-
12 sources necessary to implement the Strategy, includ-
13 ing specific budgetary requests.

14 (19) A description of such legislative or admin-
15 istrative action as may be necessary to carry out the
16 Strategy.

17 (e) LIMITATION.—

18 (1) IN GENERAL.—The Strategy shall not in-
19 clude a recommendation or a proposal to nationalize
20 5th or future generations wireless communications
21 systems or infrastructure.

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

1 (A) conduct cybersecurity incident, threat,
2 or asset response and recovery activities;

3 (B) obtain or execute warrants or other in-
4 vestigative or intelligence tools; or

5 (C) provide assistance to a private entity
6 upon request of the entity.

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

11 (g) BRIEFING.—

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

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

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

24 (1) act as the executive agent to coordinate im-
25 plementation of the Strategy; and

- 1 (2) keep congressional committees apprised of
2 progress on implementation.
- 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.”.

