

**Calendar No. 395**116<sup>TH</sup> CONGRESS  
1<sup>ST</sup> SESSION**S. 893****[Report No. 116-184]**

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 SENATE OF THE UNITED STATES**

MARCH 27, 2019

Mr. CORNYN (for himself, Mr. BURR, Mr. WARNER, Ms. COLLINS, Mr. RUBIO, Mr. BENNET, Mr. COTTON, Mrs. FEINSTEIN, Mrs. BLACKBURN, Mr. MURPHY, and Mr. SULLIVAN) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

DECEMBER 19, 2019

Reported by Mr. WICKER, with an amendment

[Strike out all after the enacting clause and insert the part printed in *italic*]

---

**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 telecommuni-

cations 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 MOBILE TELECOMMUNICATIONS**  
 8 **SYSTEMS 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 Select Committee on Intelligence, the  
 13 Committee on Commerce, Science, and Transpor-  
 14 tation, the Committee on Foreign Relations, the  
 15 Committee on Armed Services, and the Committee  
 16 on Homeland Security and Governmental Affairs of  
 17 the Senate; and

18 (2) the Permanent Select Committee on Intel-  
 19 ligence, the Committee on Energy and Commerce,  
 20 the Committee on Foreign Affairs, the Committee  
 21 on Armed Services, and the Committee on Home-  
 22 land Security of the House of Representatives.

23 (b) **STRATEGY REQUIRED.**—Not later than 180 days  
 24 after the date of the enactment of this Act, the President,

1 in consultation with the Chairman of the Federal Commu-  
2 nications Commission, the Administrator of the National  
3 Telecommunications and Information Administration, the  
4 Secretary of Homeland Security, the Director of National  
5 Intelligence, the Attorney General, and the Secretary of  
6 Defense, shall develop and submit to the appropriate com-  
7 mittees of Congress a strategy—

8           (1) to ensure the security of 5th and future  
9           generations mobile telecommunications systems and  
10          infrastructure within the United States;

11          (2) to assist mutual defense treaty allies of the  
12          United States, strategic partners of the United  
13          States, and other countries, when in the security in-  
14          terests of the United States, in maximizing the secu-  
15          rity of 5th and future generations mobile tele-  
16          communications systems and infrastructure inside  
17          their countries; and

18          (3) to protect the competitiveness of United  
19          States companies, privacy of United States con-  
20          sumers, and integrity of standards setting bodies  
21          against political influence.

22          (c) DESIGNATION.—The strategy developed under  
23          subsection (b) shall be known as the “Secure Next Genera-  
24          tion Mobile Communications Strategy”.

1 (d) ELEMENTS.—The strategy required by subsection  
2 (b) shall represent a whole-of-government approach and  
3 shall include the following:

4 (1) A description of United States national and  
5 economic security interests pertaining to the deploy-  
6 ment of 5th and future generations mobile tele-  
7 communications 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 mobile telecommunications systems and  
13 infrastructure.

14 (3) A list of available domestic suppliers of 5th  
15 and future generations telecommunications equip-  
16 ment and other suppliers in countries that are mu-  
17 tual defense allies or strategic partners of the  
18 United States and a strategy to assess their ability  
19 to produce and supply 5th generation and future  
20 generations telecommunications systems and infra-  
21 structure.

22 (4) Identification of trusted supplier entities  
23 from both inside and outside the United States that  
24 are capable of producing and supplying to private in-  
25 dustry infrastructure and systems equipment sup-

1 porting 5th and future generations mobile tele-  
2 communications systems and infrastructure.

3 (5) Identification of where security gaps exist in  
4 the United States domestic or mutual defense treaty  
5 allies and strategic partners telecommunications  
6 equipment supply chain for 5th and future genera-  
7 tions infrastructure and systems equipment.

8 (6) Identification of incentives and policy op-  
9 tions to help close or narrow such security gaps in  
10 the United States domestic industrial base, including  
11 research and development in critical technologies  
12 and workforce development in new generation tech-  
13 nologies.

14 (7) Identification of incentives and policy op-  
15 tions for leveraging the telecommunications equip-  
16 ment suppliers from mutual defense treaty allies,  
17 strategic partners, and other countries to ensure  
18 that private industry in the United States has ade-  
19 quate sources for secure, effective, and reliable 5th  
20 and future generations mobile telecommunications  
21 systems and infrastructure equipment.

22 (8) A strategy for diplomatic engagement with  
23 mutual defense treaty allies, strategic partners, and  
24 other countries to share security risk information  
25 and findings pertaining to 5th and future genera-

1        tions mobile telecommunications systems and infra-  
2        structure equipment and cooperation on mitigating  
3        those risks.

4            (9) A strategy for engagements with private  
5        sector telecommunications infrastructure and sys-  
6        tems equipment developers to share information and  
7        findings on 5th and future generations mobile tele-  
8        communication systems and infrastructure equip-  
9        ment standards to secure platforms.

10           (10) A strategy for diplomatic engagements  
11        with mutual defense treaty allies, strategic partners,  
12        and other countries to share information and find-  
13        ings on 5th and future generations mobile tele-  
14        communication systems and infrastructure equip-  
15        ment standards and standards setting bodies to pro-  
16        mote maximum interoperability, competitiveness,  
17        openness, and secure platforms.

18           (11) A strategy for joint testing environments  
19        with mutual defense treaty allies, strategic partners,  
20        and other countries to ensure a trusted marketplace  
21        for 5th and future generations mobile telecommuni-  
22        cation systems and infrastructure equipment.

23           (12) A strategy for research and development  
24        by the Federal Government, in close partnership  
25        with trusted supplier entities, mutual defense treaty

1 allies, strategic partners, and other countries to  
2 reach and maintain United States leadership in 5th  
3 and future generations communications security, in-  
4 cluding the development of an ongoing monitoring  
5 capability of 5th and future generations tele-  
6 communications systems for security vulnerabilities.

7 (13) Options for identifying and helping to  
8 mitigate the security risks of 5th and future genera-  
9 tions telecommunications systems and infrastructure  
10 equipment with security flaws or vulnerabilities or  
11 equipment sourced from countries of concern that  
12 have already been put in place within mutual de-  
13 fense treaty allies, strategic partners, and other  
14 countries, when in the security interests of the  
15 United States.

16 (14) A description of the appropriate roles and  
17 missions of the Federal Communications Commis-  
18 sion, the National Telecommunications and Informa-  
19 tion Administration, the Department of Homeland  
20 Security, the intelligence community, the Depart-  
21 ment of Justice, and the Department of Defense in  
22 executing the strategy.

23 (15) Development of a plan that includes inter-  
24 agency mechanisms for the National Telecommuni-  
25 cations and Information Administration to act as the

1 executive agent to coordinate implementation of the  
2 strategy.

3 (16) An identification of the key diplomatic, de-  
4 velopment, intelligence, military, and economic re-  
5 sources necessary to implement the strategy, includ-  
6 ing specific budgetary requests.

7 (17) A description of such legislative or admin-  
8 istrative action as may be necessary to carry out the  
9 strategy.

10 (e) LIMITATION.—The strategy required by sub-  
11 section (b) shall not include a recommendation or a pro-  
12 posal to Federalize 5th or future generations mobile tele-  
13 communications systems or infrastructure.

14 (f) BRIEFING.—Not later than 14 days after the date  
15 on which the strategy required by subsection (b) is com-  
16 pleted, the President's designee shall provide to the appro-  
17 priate committees of Congress a briefing on the implemen-  
18 tation of the strategy.

19 (g) IMPLEMENTATION.—The National Telecommuni-  
20 cations and Information Administration shall act as the  
21 executive agent to coordinate implementation of the strat-  
22 egy, and keep congressional committees apprised of  
23 progress on implementation.

1       (h) ~~FORM.~~—The strategy submitted under subsection  
 2 (b) shall be submitted in unclassified form, but may in-  
 3 clude a classified annex.

4 **SECTION 1. SHORT TITLE.**

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

7 **SEC. 2. STRATEGY TO ENSURE SECURITY OF NEXT GENERA-**  
 8 **TION WIRELESS COMMUNICATIONS SYSTEMS**  
 9 **AND INFRASTRUCTURE.**

10       (a) *APPROPRIATE COMMITTEES OF CONGRESS DE-*  
 11 *FINED.*—*In this section, the term “appropriate committees*  
 12 *of Congress” means—*

13               (1) *the Select Committee on Intelligence, the*  
 14 *Committee on Commerce, Science, and Transpor-*  
 15 *tation, the Committee on Foreign Relations, the Com-*  
 16 *mittee on Armed Services, and the Committee on*  
 17 *Homeland Security and Governmental Affairs of the*  
 18 *Senate; and*

19               (2) *the Permanent Select Committee on Intel-*  
 20 *ligence, the Committee on Energy and Commerce, the*  
 21 *Committee on Foreign Affairs, the Committee on*  
 22 *Armed Services, and the Committee on Homeland Se-*  
 23 *curity of the House of Representatives.*

24       (b) *STRATEGY REQUIRED.*—*Not later than 180 days*  
 25 *after the date of the enactment of this Act, the President,*

1 *in consultation with the Chairman of the Federal Commu-*  
2 *nications Commission, the Assistant Secretary of Commerce*  
3 *for Communications and Information, the Secretary of*  
4 *Homeland Security, the Director of National Intelligence,*  
5 *the Attorney General, and the Secretary of Defense, shall*  
6 *develop and submit to the appropriate committees of Con-*  
7 *gress a strategy—*

8           (1) *to ensure the security of 5th and future gen-*  
9 *erations wireless communications systems and infra-*  
10 *structure within the United States;*

11           (2) *to provide technical assistance to mutual de-*  
12 *fense treaty allies of the United States, strategic part-*  
13 *ners of the United States, and other countries, when*  
14 *in the security interests of the United States, to maxi-*  
15 *mize the security of 5th and future generations wire-*  
16 *less communications systems and infrastructure in-*  
17 *side their countries; and*

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

23           (c) *DESIGNATION.*—*The strategy developed under sub-*  
24 *section (b) shall be known as the “Secure Next Generation*

1 *Wireless Communications Strategy*” (referred to in this sec-  
2 *tion as the “Strategy”).*

3 (d) *ELEMENTS.—The Strategy shall represent a whole-*  
4 *of-government approach and shall include the following:*

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

9 (2) *An identification and assessment of potential*  
10 *security threats and vulnerabilities to the infrastruc-*  
11 *ture, equipment, systems, software, and virtually de-*  
12 *finied networks that support 5th and future genera-*  
13 *tions wireless communications systems and infra-*  
14 *structure. The assessment shall include a comprehen-*  
15 *sive evaluation of the full range of threats to, and*  
16 *unique security challenges posed by, 5th and future*  
17 *generations wireless communications systems and in-*  
18 *frastructure, as well as steps that public and private*  
19 *sector entities can take to mitigate those threats.*

20 (3) *An identification and assessment of the glob-*  
21 *al competitiveness and vulnerabilities of United*  
22 *States manufacturers and suppliers of 5th and future*  
23 *generations wireless communications equipment.*

24 (4) *A list of available domestic suppliers of 5th*  
25 *and future generations wireless communications*

1        *equipment and other suppliers in countries that are*  
2        *mutual defense allies or strategic partners of the*  
3        *United States and a strategy to assess their ability to*  
4        *produce and supply 5th generation and future genera-*  
5        *tions wireless communications systems and infra-*  
6        *structure.*

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

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

18                *(7) Identification of incentives and policy op-*  
19        *tions to help close or narrow any security gaps iden-*  
20        *tified under paragraph (6) in, and ensure the eco-*  
21        *nommic viability of, the United States domestic indus-*  
22        *trial base, including research and development in*  
23        *critical technologies and workforce development in 5th*  
24        *and future generations wireless communications sys-*  
25        *tems and infrastructure.*

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

9           (9) *A strategy for diplomatic engagement with*  
10          *mutual defense treaty allies, strategic partners, and*  
11          *other countries to share security risk information and*  
12          *findings pertaining to 5th and future generations*  
13          *wireless communications systems and infrastructure*  
14          *equipment and cooperation on mitigating those risks.*

15          (10) *A strategy for engagement with private sec-*  
16          *tor communications infrastructure and systems equip-*  
17          *ment developers to share information and findings on*  
18          *5th and future generations wireless communications*  
19          *systems and infrastructure equipment standards to*  
20          *secure platforms.*

21          (11) *A strategy for engagement with private sec-*  
22          *tor communications infrastructure and systems equip-*  
23          *ment developers to encourage the maximum partici-*  
24          *pation possible on standards-setting bodies related to*  
25          *such systems and infrastructure equipment standards*

1 *by public and private sector entities from the United*  
2 *States.*

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

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

19 *(14) A strategy for joint testing environments*  
20 *with mutual defense treaty allies, strategic partners,*  
21 *and other countries to ensure a trusted marketplace*  
22 *for 5th and future generations wireless communica-*  
23 *tions systems and infrastructure equipment.*

24 *(15) A strategy for research and development by*  
25 *the Federal Government, in close partnership with*

1 *trusted supplier entities, mutual defense treaty allies,*  
2 *strategic partners, and other countries to reach and*  
3 *maintain United States leadership in 5th and future*  
4 *generations wireless communications systems and in-*  
5 *frastructure security, including the development of an*  
6 *ongoing monitoring capability of 5th and future gen-*  
7 *erations wireless communications systems to identify*  
8 *security vulnerabilities.*

9 *(16) Options for identifying and helping to miti-*  
10 *gate the security risks of 5th and future generations*  
11 *wireless communications systems and infrastructure*  
12 *that have security flaws or vulnerabilities, or are uti-*  
13 *lizing equipment sourced from countries of concern,*  
14 *and that have already been put in place within the*  
15 *systems and infrastructure of mutual defense treaty*  
16 *allies, strategic partners, and other countries, when in*  
17 *the security interests of the United States.*

18 *(17) Development of a plan that includes a de-*  
19 *scription of the roles and responsibilities of the appro-*  
20 *priate executive branch agencies and interagency*  
21 *mechanisms for the Assistant Secretary of Commerce*  
22 *for Communications and Information to act as the*  
23 *executive agent to coordinate implementation of the*  
24 *Strategy, as provided in subsection (g).*

1           (18) *An identification of the key diplomatic, de-*  
2 *velopment, intelligence, military, and economic re-*  
3 *sources necessary to implement the Strategy, includ-*  
4 *ing specific budgetary requests.*

5           (19) *A description of such legislative or adminis-*  
6 *trative action as may be necessary to carry out the*  
7 *Strategy.*

8       (e) *LIMITATIONS.—*

9           (1) *IN GENERAL.—The Strategy shall not include*  
10 *a recommendation or a proposal to nationalize 5th or*  
11 *future generations wireless communications systems*  
12 *or infrastructure.*

13          (2) *FEDERAL AGENCY AUTHORITY.—Nothing in*  
14 *this section shall be construed to limit the authority*  
15 *or ability of a Federal agency to—*

16               (A) *conduct cybersecurity incident, threat,*  
17 *or asset response and recovery activities;*

18               (B) *obtain or execute warrants or other in-*  
19 *vestigative or intelligence tools; or*

20               (C) *provide assistance to a private entity*  
21 *upon request of the entity.*

22       (f) *BRIEFING.—*

23           (1) *IN GENERAL.—Not later than 14 days after*  
24 *the date on which the Strategy is completed, the As-*  
25 *stant Secretary of Commerce for Communications*

1        *and Information, and any other Federal officials des-*  
2        *ignated by the President, shall provide to the appro-*  
3        *priate committees of Congress a briefing on the imple-*  
4        *mentation of the Strategy.*

5                (2) *UNCLASSIFIED SETTING.*—*The briefing under*  
6        *paragraph (1) shall be held in an unclassified setting*  
7        *to the maximum extent possible.*

8                (g) *IMPLEMENTATION.*—*The Assistant Secretary of*  
9        *Commerce for Communications and Information shall—*

10                (1) *act as the executive agent to coordinate im-*  
11        *plementation of the Strategy; and*

12                (2) *keep congressional committees apprised of*  
13        *progress on implementation.*

14                (h) *FORM.*—*The Strategy shall be submitted to the ap-*  
15        *propriate committees of Congress in unclassified form, but*  
16        *may include a classified annex.*

Calendar No. 395

116<sup>TH</sup> CONGRESS  
1<sup>ST</sup> Session

**S. 893**

[Report No. 116-184]

---

---

## **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.

---

---

DECEMBER 19, 2019

Reported with an amendment