Calendar No. 395

116TH CONGRESS *1st Session*	SENATE	REPORT 116–184

SECURE 5G AND BEYOND ACT OF 2019

R E P O R T

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ON

S. 893

DECEMBER 19, 2019.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE

99–010 WASHINGTON : 2019

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

ROGER F. WICKER, Mississippi, *Chairman*

JOHN THUNE, South Dakota
ROY BLUNT, Missouri
TED CRUZ, Texas
DEB FISCHER, Nebraska
JERRY MORAN, Kansas
DAN SULLIVAN, Alaska
CORY GARDNER, Colorado
MARSHA BLACKBURN, Tennessee
SHELLEY MOORE CAPITO, West Virginia
MIKE LEE, Utah
RON JOHNSON, Wisconsin
TODD C. YOUNG, Indiana
RICK SCOTT, Florida

MARIA CANTWELL, Washington
AMY KLOBUCHAR, Minnesota
RICHARD BLUMENTHAL, Connecticut
BRIAN SCHATZ, Hawaii
EDWARD J. MARKEY, Massachusetts
TOM UDALL, New Mexico
GARY C. PETERS, Michigan
TAMMY BALDWIN, Wisconsin
TAMMY DUCKWORTH, Illinois
JON TESTER, Montana
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada

JOHN KEAST, *Staff Director*
DAVID STRICKLAND, *Minority Staff Director*

Calendar No. 395

116TH CONGRESS *1st Session* | SENATE | REPORT 116–184

SECURE 5G AND BEYOND ACT OF 2019

DECEMBER 19, 2019.—Ordered to be printed

Mr. WICKER, from the Committee on Commerce, Science, and Transportation, submitted the following

R E P O R T

[To accompany S. 893]

[Including cost estimate of the Congressional Budget Office]

The Committee on Commerce, Science, and Transportation, to which was referred the bill (S. 893) 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, having considered the same, reports favorably thereon with an amendment (in the nature of a substitute) and recommends that the bill (as amended) do pass.

PURPOSE OF THE BILL

The purpose of S. 893, the Secure 5G and Beyond Act of 2019, is to require the President to develop a strategy to ensure the security of 5th generation (5G) and other future generations of wireless communications systems and infrastructure in the United States, and to assist allies in maximizing the security of their 5G and other future generations of wireless communications systems and infrastructure, and software.

BACKGROUND AND NEEDS

The United States and some other countries have concluded that Chinese communications equipment vendors Huawei and ZTE pose

a national security risk,[1] because Chinese law requires organizations and citizens to "support, cooperate with, and collaborate in national intelligence work."[2] U.S. communications providers have been urged to remove Huawei and ZTE equipment from their networks to prevent cyberattacks and other threats to the stability and reliability of the Nation's communications systems.[3] As early as 2012, a report issued by the Permanent Select Committee on Intelligence of the House of Representatives warned of the national security threat posed by Huawei and ZTE.[4]

In 2018, Congress barred Federal agencies from procuring communications services from providers that have purchased equipment from Huawei and ZTE, and also limited the ability of the Federal Government to provide grants, loans, and loan guarantees to providers who intend to use that money to purchase equipment from those same providers.[5] On May 15, 2019, President Trump issued an Executive order prohibiting the "acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service . . . where the transaction involves any property in which any foreign country or a national thereof has any interest. . . ."[6] On November 22, 2019, the Federal Communications Commission (FCC or Commission) approved a prohibition on the use of universal service funds to purchase equipment or services from any communications equipment or service providers identified as posing a national security risk to communications networks or the communications supply chain.[7] The Commission also recently denied an application by China Mobile to provide international telecommunications services between the United States and foreign destinations, citing "China Mobile USA's ownership and control by the Chinese Government."[8]

The U.S. Government and allies are taking steps to help protect their communications networks from potential risks posed by Huawei and ZTE equipment and services.[9] Australia and New Zea-

---

[1] See, e.g., Executive Order on Securing the Information and Communications Technology and Services Supply Chain, May 15, 2019, Executive order (*https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/*); see also, Michael Kahn and Jan Lopatka, "Western Allies Agree 5G Security Guidelines Warn of Outside Influence," Reuters, May 3, 2019 (*https://www.reuters.com/article/us-telecoms-5g-security/western-allies-agree-5g-security-guidelines-warn-of-outside-influence-idUSKCN1S91D2*).

[2] Michael Kahn and Jan Lopatka, "Western Allies Agree 5G Security Guidelines Warn of Outside Influence," Reuters, May 3, 2019 (*https://www.reuters.com/article/us-telecoms-5g-security/western-allies-agree-5g-security-guidelines-warn-of-outside-influence-idUSKCN1S91D2*).

[3] Tom Cotton and John Cornyn, "Keep the Chinese Government Away From 5G Technology," Washington Post, April 1, 2019 (*https://www.washingtonpost.com/opinions/keep-the-chinese-government-away-from-5g-technology/2019/04/01/ba7a30ac-54b3-11e9-9136-f8e636f1f6df_story.html?utm_term=.055accd882e0*).

[4] U.S. Permanent Select Committee on Intelligence, "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," October 8, 2012 (*https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=96*).

[5] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115–232, sec. 889.

[6] Executive Order 13873 (*https://www.Federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply chain*).

[7] Federal Communications Commission, press release, FCC Bars Use of Universal Service Funding for Equipment & Services Posing National Security Risks, November 22, 2019 (*https://docs.fcc.gov/public/attachments/DOC-360976A1.pdf*).

[8] In the Matter of China Mobile International (USA) Inc., Application for Global Facilities-Based and Global Resale International Telecommunications Authority Pursuant to Section 214 of the Communications Act of 1934, as Amended, ITC–210–20110901–00289, Memorandum Opinion and Order, FCC 19–38, released May 10, 2019, China Mobile Order (*https://docs.fcc.gov/public/attachments/FCC-19-38A1.pdf*).

[9] Lenka Ponikelska, "Countries Seek United 5G Security Approach Amid Huawei Concerns," Bloomberg, May 3, 2019 (*https://www.bloomberg.com/news/articles/2019-05-03/countries-seek-united-5g-security-approach-amid-huawei-concerns*).

land have blocked the use of Huawei to provide the technology for their 5G networks.[10] Japan has effectively banned Huawei and ZTE from official contracts, with its top three telecom operators following suit.[11] Canada is reviewing its relationship with Huawei.[12] The United Kingdom's National Cyber Security Centre has warned of the potential threats,[13] and British Telecom is removing Huawei equipment from key areas of its 4G network and will not use Huawei in central parts of its 5G network.[14]

Yet although there is significant international concern about the national security implications of the use of Huawei and ZTE equipment, not all countries have limited the use of those companies' equipment in their domestic communications networks.[15] Furthermore, there is concern about the availability of alternative secure communications infrastructure and software for use in U.S. and international wireless networks.[16] Many have argued it would be helpful for the Federal Government to develop a single unified strategy for how to deal with the national security implications related to Huawei and ZTE, both within domestic communications networks and in the Nation's international diplomatic relationships.[17]

---

[10] "Huawei: Should We Be Worried About the Chinese Tech Giant?," BBC, March 7, 2019 (*https://www.bbc.com/news/business-46465438*).

[11] Simon Denyer, "Japan Effectively Bans China's Huawei and ZTE From Government Contracts, Joining U.S.," Washington Post, December 10, 2018 (*https://www.washingtonpost.com/world/asia_pacific/japan-effectively-bans-chinas-huawei-zte-from-government-contracts-joining-us/2018/12/10/748fe98a-fc69-11e8-ba87-8c7facdf6739_story.html?utm_term=.b9e4d0a33b28*).

[12] "Huawei: Should We Be Worried About the Chinese Tech Giant?," BBC, March 7, 2019 (*https://www.bbc.com/news/business-46465438*).

[13] Alistair Bunkall, "Huawei: Chinese Telecoms Giant 'Still A Security Threat to UK'—GCHQ," SkyNews, March 28, 2019 (*https://news.sky.com/story/huawei-chinese-telecoms-giant-still-a-security-threat-to-uk-gchq-11677162*).

[14] "Huawei: Should We Be Worried About the Chinese Tech Giant?," BBC, March 7, 2019 (*https://www.bbc.com/news/business-46465438*); see also Alex Hern, "BT Removing Huawei Equipment From Parts of 4G Network," The Guardian, December 5, 2018 (*https://www.theguardian.com/technology/2018/dec/05/bt-removing-huawei-equipment-from-parts-of-4g-network*).

[15] See Alexander Cornwell, "Bahrain to Use Huawei in 5G Rollout Despite U.S. Warnings," Reuters, March 26, 2019 (*https://www.reuters.com/article/us-huawei-security-bahrain/bahrain-to-use-huawei-in-5g-rollout-despite-us-warnings-idUSKCN1R71B3*); see Philip Blenkinsop, "Belgian Cybersecurity Agency Finds No Threat From Huawei," Reuters, April 15, 2019 (*https://www.reuters.com/article/us-huawei-tech-security-belgium/belgian-cybersecurity-agency-finds-no-threat-from-huawei-idUSKCN1RR1GP*); see Mathieu Rosemain, Gwenaelle Barzic and Elizabeth Pineau, "French Senate Rejects Tougher Telecoms Controls Despite U.S. Huawei Warning," Reuters, February 6, 2019 (*https://www.reuters.com/article/us-huawei-europe-france/french-senate-rejects-tougher-telecoms-controls-despite-u-s-huawei-warning-idUSKCN1PV2B8*); see Stephen Jewkes and Giselda Vagnoni, "Italy Denies It Will Ban Huawei, ZTE From Its 5G Plans," Reuters, February 7, 2019 (*https://www.reuters.com/article/us-huawei-europe-italy/italy-denies-it-will-ban-huawei-zte-from-its-5g-plans-idUSKCN1PW0LV*); see Victoria Klesty, "Norway Will Not Ban Huawei From 5G Mobile Network: Minister," Reuters, September 26, 2019 (*https://www.reuters.com/article/us-norway-huawei-tech/norway-will-not-ban-huawei-from-5g-mobile-network-minister-idUSKBN1WB15G*); see Patpicha Tanakasempipat, "Thailand Launches Huawei 5G Test Bed, Even as U.S. Urges Allies To Bar Chinese Gear," Reuters, February 8, 2019 (*https://www.reuters.com/article/us-huawei-thailand/thailand-launches-huawei-5g-test-bed-even-as-u-s-urges-allies-to-bar-chinese-gear-idUSKCN1PX0DY*); see Alexander Cornwell, "U.S. Flags Huawei 5G Network Security Concerns to Gulf Allies," Reuters, September 12, 2019 (*https://www.reuters.com/article/us-huawei-security-usa-gulf/u-s-flags-huawei-5g-network-security-concerns-to-gulf-allies-idUSKCN1VX241*); see Alexander Cornwell, "UAE's Du Says U.S. Ban on Huawei Not an Issue for 5G Network," Reuters, July 24, 2019 (*https://www.reuters.com/article/us-huawei-security-du/uaes-du-says-u-s-ban-on-huawei-not-an-issue-for-5g-network-idUSKCN1UJ13I*).

[16] See Brian Fung, "How China's Huawei Took the Lead Over U.S. Companies in 5G Technology," The Washington Post, April 10, 2019 (*https://www.washingtonpost.com/technology/2019/04/10/us-spat-with-huawei-explained/*); see Eric Jhonsa, "Huawei's Work on Alternatives to U.S. Tech—And the Challenges They Face," Real Money, August 30, 2019 (*https://realmoney.thestreet.com/investing/technology/huawei-s-work-on-alternatives-to-u-s-tech-and-the-challenges-they-face-15072796*).

[17] See Jacqueline Thomsen, "Key Senators Say Administration Should Ban Huawei Tech in US Electric Grid," The Hill, February 25, 2019 (*https://thehill.com/policy/cybersecurity/*

Continued

SUMMARY OF PROVISIONS

S. 893 would do the following:

- Require the President of the United States to develop a Federal Government-wide strategy to ensure the security of the Nation's next-generation—and future generations—wireless telecommunications systems and infrastructure.
- Direct the U.S. Government to assist allies and strategic partners in maximizing the security of next-generation wireless telecommunications systems, infrastructure, and software.

LEGISLATIVE HISTORY

S. 893 was introduced on March 27, 2019, by Senator Cornyn (for himself and Senators Burr, Warner, Collins, Rubio, Bennet, Cotton, and Feinstein) and was referred to the Senate Committee on Commerce, Science, and Transportation of the Senate. Senators Blackburn, Murphy, and Sullivan are additional cosponsors. On July 24, 2019, the Committee met in open Executive Session and, by voice vote, ordered S. 893 reported favorably with an amendment (in the nature of a substitute) offered by Senator Wicker. The Committee also adopted two additional amendments related to the bill. The first, offered by Senator Lee, would provide that the strategy developed pursuant to the bill shall include the provision of technical assistance to other countries to maximize the security of 5th and future generations wireless communications systems and infrastructure. The second, offered by Senator Cruz, would require that the strategy include identification and assessment of the global competitiveness and vulnerabilities of United States manufacturers and suppliers of 5th and future generations wireless communications equipment, and identify incentives and policy options to ensure the economic viability of the U.S. domestic industrial base.

Similar legislation, H.R. 2881, is pending in the House of Representatives. On May 21, 2019, H.R. 2881 was introduced by Representative Spanberger (D–VA) (for herself and Representatives Stefanik (R–NY), Slotkin (D–MI), Rooney (R–FL), O'Halleran (D–AZ), and Brooks (R–IN)) and was referred to the Committees on Energy and Commerce, and Foreign Affairs of the House of Representatives.

ESTIMATED COSTS

In accordance with paragraph 11(a) of rule XXVI of the Standing Rules of the Senate and section 403 of the Congressional Budget Act of 1974, the Committee provides the following cost estimate, prepared by the Congressional Budget Office:

431427-senators-request-trump-admin-consider-ban-on-huawei-tech-in-us-electric); see Adam Segal, "The Right Way to Deal With Huawei: The United States Needs to Compete With Chinese Firms, Not Just Ban Them," Foreign Affairs, July 11, 2019 (*https://www.foreignaffairs.com/articles/china/2019-07-11/right-way-deal-huawei*).

S. 893, Secure 5G and Beyond Act of 2019

As ordered reported by the Senate Committee on Commerce, Science, and Transportation on July 24, 2019

Millions of Dollars	2019	2019-2024	2019-2029
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Deficit Effect	0	0	0
Spending Subject to Appropriation (Outlays)	0	1	not estimated

		Mandate Effects	
Pay-as-you-go procedures apply?	No	Contains intergovernmental mandate?	No
Increases on-budget deficits in any of the four consecutive 10-year periods beginning in 2030?	No	Contains private-sector mandate?	Yes, Under Threshold

S. 893 would require the President, acting through the National Telecommunications and Information Administration (NTIA) and other federal agencies, to develop and submit to the Congress a strategy to ensure the security of 5G and future generations wireless communications systems and infrastructure owned by the United States and its allies. Among various other requirements, the NTIA would have to assess potential security threats to American 5G systems and infrastructure and analyze how competitive American 5G manufacturers and suppliers are globally.

Using information from the NTIA, CBO estimates that implementing S. 893 would cost $1 million for the interagency group to formulate the strategy. Such spending would be subject to the availability of appropriated funds. CBO expects that NTIA would coordinate the interagency group and complete the strategy in 2020. The Federal Communications Commission (FCC) would incur insignificant costs to help formulate the strategy. However, because the FCC is authorized under current law to collect fees sufficient to offset the appropriated costs of its regulatory activities each year, CBO estimates that the net cost to the FCC would be negligible, assuming appropriation actions consistent with that authority.

If the FCC increases annual fee collections to offset the costs of implementing provisions in the bill, S. 893 would increase the cost of an existing private-sector mandate on entities required to pay those fees. Using information from the FCC, CBO estimates that the incremental cost of the mandate would be small and would fall well below the annual threshold established in the Unfunded Mandates Reform Act (UMRA) for private-sector mandates ($164 million in 2019, adjusted annually for inflation).

The bill contains no intergovernmental mandates as defined in UMRA.

The CBO staff contacts for this estimate are David Hughes (for federal costs) and Rachel Austin (for mandates). The estimate was reviewed by H. Samuel Papenfuss, Deputy Assistant Director for Budget Analysis.

REGULATORY IMPACT STATEMENT

In accordance with paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee provides the following evaluation of the regulatory impact of the legislation, as reported:

NUMBER OF PERSONS COVERED

The number of persons covered by S. 893 would be consistent with current levels. S. 893 would have no effect on the number or types of individuals and businesses regulated.

ECONOMIC IMPACT

S. 893 would have no economic impact. By promoting more secure deployment of next-generation communications throughout the United States and the world, the bill would allow the Nation to extend its technology leadership in the next generation of communications technology and promote investment and innovation.

PRIVACY

S. 893 would not have any adverse impact on the personal privacy of affected individuals.

PAPERWORK

The Committee does not anticipate a major increase in paperwork burdens resulting from the passage of this legislation. The bill, as reported, would direct a broad group of Federal stakeholders to prepare a whole-of-government strategy concerning the security of 5th and future generations wireless communications systems and infrastructure and various other issues. The bill would direct the stakeholders to prepare and submit a report to Congress outlining the strategy within 180 days of the enactment of the bill.

CONGRESSIONALLY DIRECTED SPENDING

In compliance with paragraph 4(b) of rule XLIV of the Standing Rules of the Senate, the Committee provides that no provisions contained in the bill, as reported, meet the definition of congressionally directed spending items under the rule.

SECTION-BY-SECTION ANALYSIS

Section 1. Short title

This section would provide that the bill may be cited as the "Secure 5G and Beyond Act of 2019".

Section 2. Strategy to ensure security of next generation wireless communications systems and infrastructure

Subsection (a) of this section would define the term "appropriate committees of Congress" for purposes of the bill.

Subsections (b) and (c) of this section would require the President, in consultation with various other Federal officials, to develop and submit to the appropriate committees of Congress within 180 days of enactment a "Secure Next Generation Wireless Communications Strategy" to do the following:

- Ensure the security of 5th generation (5G) and future generations of U.S. wireless communications systems and infrastructure.
- Provide technical assistance to U.S. mutual defense treaty allies, strategic partners, and other countries, when in the security interests of the United States, to maximize the security of 5G and future generations of wireless communications systems and infrastructure inside their countries.
- Protect the competitiveness of U.S. companies, the privacy of U.S. consumers, and the integrity and impartiality of standards-setting bodies related to 5G and future generations of wireless communications systems and infrastructure.

Subsection (d) of this section would require that the strategy represent a whole-of-government approach to the issues set forth in section 2(b). The subsection then outlines 19 elements that would need to be included in the strategy as follows:

(1) A description of U.S. national and economic security interests pertaining to the deployment of 5G and future generations of wireless communications systems and infrastructure.

(2) An identification and assessment of potential security threats and vulnerabilities to the infrastructure, equipment, systems, software, and virtually defined networks that support 5G and future generations of wireless communications systems and infrastructure. This assessment would also include a comprehensive evaluation of the full range of threats to, and unique security challenges posed by such systems and infrastructure, as well as steps that public and private sector entities can take to mitigate such threats. The Committee intends for this evaluation to include a detailed discussion of the cybersecurity issues posed by the deployment and use of such systems and infrastructure.

(3) An identification and assessment of the global competitiveness and vulnerabilities of U.S. manufacturers and suppliers of 5G and future generations of wireless communications equipment.

(4) A list of domestic suppliers of 5G and future generations of wireless communications equipment and other suppliers in countries that are mutual defense allies or strategic partners as well as a strategy to assess their ability to produce and supply such systems and infrastructure.

(5) Identification of trusted supplier entities from both inside and outside of the United States that are capable of producing and supplying to private industry infrastructure and systems equipment supporting 5G and future generations of wireless communications systems and infrastructure.

(6) Identification of where security gaps exist in the domestic or mutual defense treaty allies and strategic partner communications equipment supply chain for 5G and future generations wireless communications systems and infrastructure.

(7) Identification of incentives and policy options to help close or narrow any security gaps in, and ensure the economic viability of, the U.S. domestic industrial base, including research and development in critical technologies and workforce development in 5G and future generations wireless communications systems and infrastructure.

(8) Identification of incentives and policy options for leveraging the communications equipment suppliers from mutual defense trea-

ty allies, strategic partners, or other countries to ensure that U.S. private industry has adequate sources for secure, effective, and reliable 5G and future generations of wireless communications systems and infrastructure equipment.

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

(10) A strategy for engagement with private sector communications infrastructure and systems equipment developers to share information and findings on 5G and future generations wireless communications systems and infrastructure equipment standards to secure platforms.

(11) A strategy for engagement with private sector communications infrastructure and systems equipment developers to encourage the maximum participation possible on standards-setting bodies related to such systems and infrastructure equipment standards by U.S. public and private sector entities.

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

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

(14) A strategy for joint testing environments with mutual defense treaty allies, strategic partners, and other countries to ensure a trusted marketplace for 5G and future generations wireless communications systems and infrastructure equipment.

(15) A strategy for research and development by the Federal Government, in close partnership with trusted supplier entities, mutual defense treaty allies, strategic partners, and other countries to reach and maintain U.S. leadership in 5G and future generations wireless communications systems and infrastructure security, including the development of an ongoing monitoring capability for such systems to identify security vulnerabilities.

(16) Options for identifying and helping to mitigate the security risks of 5G and future generations wireless communications systems and infrastructure that have security flaws or vulnerabilities, or are utilizing equipment sourced from countries of concern, and that have already been put in place within the systems and infrastructure of mutual defense treaty allies, strategic partners, and other countries, when in U.S. security interests.

(17) Development of a plan that includes a description of the appropriate roles and responsibilities of the appropriate executive branch agencies and interagency mechanisms for the National Telecommunications and Information Administration to act as the

executive agent to coordinate implementation of the strategy consistent with section 2(g).

(18) An identification of the key diplomatic, development, intelligence, military, and economic resources necessary to implement the strategy, including specific budgetary requests.

(19) A description of such legislative or administrative action as may be necessary to carry out the strategy.

Subsection (e) of this section would prohibit the strategy from including a recommendation or proposal to federalize 5G or future generations of wireless telecommunications systems or infrastructure. This subsection would further make clear that nothing in the subsection shall be construed to limit the authority or ability of a Federal agency to do the following:

- Conduct cybersecurity incident, threat, or asset response and recovery activities;
- Obtain or execute warrants or other investigative or intelligence tools; or
- Provide assistance to a private entity upon the request of such entity.

Subsection (f) of this section would require the Assistant Secretary of Commerce for Communications and Information, and other Federal officials as designated by the President, to provide the appropriate committees of Congress with a briefing on the implementation of the strategy within 14 days of its completion. The briefing would need to be held in an unclassified setting to the maximum extent possible.

Subsection (g) of this section would designate the National Telecommunications and Information Administration as the executive agent to coordinate implementation of the strategy and keep Congress apprised of progress on implementation. The Committee intends for such coordination activity to be performed in due regard of the fact that the FCC (one of the participants in the development of the strategy) is an independent agency subject to the jurisdiction of Congress, not the executive branch.

Subsection (h) of this section would specify that the strategy must be submitted to Congress in unclassified form, but may include a classified annex.

CHANGES IN EXISTING LAW

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, the Committee states that the bill as reported would make no change to existing law.

○