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.
Be it enacted by the Senate and House of Representa-
tives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

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

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

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

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

(2) the Select Committee on Intelligence, the
Committee on Commerce, Science, and Transpor-
tation, the Committee on Foreign Relations, the
Committee on Armed Services, and the Committee
on Homeland Security and Governmental Affairs of
the Senate.

(b) STRATEGY REQUIRED.—Not later than 180 days
after the date of the enactment of this Act, the President,
in consultation with the Chairman of the Federal Commu-
The Assistant Secretary of Commerce for Communications and Information, the Secretary of Homeland Security, the Director of National Intelligence, the Attorney General, the Secretary of Defense, and the Secretary of State, shall develop and submit to the appropriate committees of Congress a strategy—

(1) to ensure the security of 5th and future generations wireless communications systems and infrastructure within the United States;

(2) to provide technical assistance to mutual defense treaty allies of the United States, strategic partners of the United States, and other countries, when in the security interests of the United States, to maximize the security of 5th and future generations wireless communications systems and infrastructure inside their countries; and

(3) to protect the competitiveness of United States companies, privacy of United States consumers, and integrity and impartiality of standards-setting bodies related to 5th and future generations wireless communications systems and infrastructure.

(c) DESIGNATION.—The strategy developed under subsection (b) shall be known as the “Secure Next Generation Wireless Communications Strategy” (referred to in this section as the “Strategy”).
(d) ELEMENTS.—The Strategy shall represent a whole-of-government approach and shall include the following:

(1) A description of United States national and economic security interests pertaining to the deployment of 5th and future generations 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 5th and future generations wireless communications systems and infrastructure. The assessment shall include a comprehensive evaluation of the full range of threats to, and unique security challenges posed by, 5th and future generations wireless communications systems and infrastructure, as well as steps that public and private sector entities can take to mitigate such threats.

(3) An identification and assessment of the global competitiveness and vulnerabilities of United States manufacturers and suppliers of 5th and future generations wireless communications equipment.
(4) A list of available domestic suppliers of 5th and future generations wireless communications equipment and other suppliers in countries that are mutual defense allies or strategic partners of the United States and a strategy to assess their ability to produce and supply 5th generation and future generations wireless communications systems and infrastructure.

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

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

(7) Identification of incentives and policy options to help close or narrow any security gaps identified under paragraph (6) in, and ensure the economic viability of, the United States domestic industrial base, including research and development in critical technologies and workforce development in
5th and future generations wireless communications systems and infrastructure.

(8) Identification of incentives and policy options for leveraging the communications equipment suppliers from mutual defense treaty allies, strategic partners, and other countries to ensure that private industry in the United States has adequate sources for secure, effective, and reliable 5th and future generations 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 5th 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 5th 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 public and private sector entities from the United States.

(12) A strategy for diplomatic engagement with mutual defense treaty allies, strategic partners, and other countries to share information and findings on 5th 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 5th and future generations wireless communications infrastructure and systems equipment concerning the standards-setting bodies related to such systems and infrastructure equipment 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 5th 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 United States leadership in 5th and future generations wireless communications systems and infrastructure security, including the development of an ongoing monitoring capability of 5th and future generations wireless communications systems to identify security vulnerabilities.

(16) Options for identifying and helping to mitigate the security risks of 5th 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 the security interests of the United States.

(17) Development of a plan that includes a description of the roles and responsibilities of the appropriate executive branch agencies and interagency
mechanisms for the Assistant Secretary of Commerce for Communications and Information to act as the executive agent to coordinate implementation of the Strategy, as provided in subsection (h).

(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.

(e) LIMITATION.—

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

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

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

(B) obtain or execute warrants or other investigative or intelligence tools; or

(C) provide assistance to a private entity upon request of the entity.
(f) PUBLIC COMMENT.—Not later than 60 days after the date of the enactment of this Act, the President shall seek public comment regarding the development and implementation of the Strategy.

(g) BRIEFING.—

(1) IN GENERAL.—Not later than 14 days after the date on which the Strategy is completed, the Assistant Secretary of Commerce for Communications and Information, and any other Federal officials designated by the President, shall provide to the appropriate committees of Congress a briefing on the implementation of the Strategy.

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

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

(1) act as the executive agent to coordinate implementation of the Strategy;

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

(3) not implement any proposal or recommendation involving spectrum licensed by the Commission unless the implementation of such pro-
posal or recommendation is first approved by the Commission.

(i) FORM.—The Strategy shall be submitted to the appropriate committees of Congress in unclassified form, 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.”