From: jean public
To: secure5G; Hall, Travis; scoops@huffpost.com
Subject: Re: secure 5G program in USA
Date: Thursday, May 28, 2020 1:04:49 PM

this should not be a Chinese product. We should not let other countries develop this. We need to ban Huwei. This comment is for the public record. We also need to know the harm that 5G can do to human bodies and brains. Please receipt. This comment is for the public record. Jean Public jeanpublic1@gmail.com

On Thu, May 28, 2020 at 11:00 AM jean public <jeanpublic1@gmail.com> wrote:

[Federal Register Volume 85, Number 103 (Thursday, May 28, 2020)]
[Notices]
[Pages 32016-32018]
From the Federal Register Online via the Government Publishing Office
[www.gpo.gov]
[FR Doc No: 2020-11398]

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

[Docket No. 200521-0144]
RIN 0660-XC047

The National Strategy to Secure 5G Implementation Plan

AGENCY: National Telecommunications and Information Administration, U.S. Department of Commerce.

ACTION: Notice; request for public comments.

SUMMARY: In accordance with the Secure 5G and Beyond Act of 2020, the National Telecommunications and Information Administration (NTIA), on behalf of the Executive Branch, is requesting comments to inform the development of an Implementation Plan for the National Strategy to Secure 5G.

DATES: Comments must be received on or before June 18, 2020.

ADDRESSES: Written comments identified by Docket No. 200521-0144 may be submitted by email to secure5G@ntia.gov. Comments submitted by email should be machine-readable and should not be copy-protected. Written comments also may be submitted by mail to the National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue NW, Room 4725, Attn: Secure 5G RFC, Washington, DC 20230.


SUPPLEMENTARY INFORMATION:

Background: On March 23, 2020, the President signed into law the
Secure 5G and Beyond Act of 2020 (Act), which
requires the development of a strategy to ensure the security of next
generation wireless communications systems and infrastructure. The
Act further requires the development of an Implementation Plan within
180 days of enactment, and lays out 18 actions to be included in this plan.

On the same day, and in fulfilment of the requirement established
by the Act, the Administration published the National Strategy to
Secure 5G (Strategy). In so doing, the Administration recognizes
both the importance of fifth generation wireless technologies (5G) to
the future prosperity and security of the United States, as well as the
risks and vulnerabilities posed by malicious actors that will seek to
exploit these technologies. The Strategy is focused on four lines of
effort: (1) Facilitating domestic 5G rollout; (2) assessing the
cybersecurity risks to and identifying core security principles of 5G
capabilities and infrastructure; (3) addressing risks to United States
economic and national security during development and deployment of 5G
infrastructure worldwide; and (4) promoting responsible global
development and deployment of secure and reliable 5G infrastructure. In
accordance with both the Act and the Strategy, the National Security
and National Economic Councils are developing an Implementation Plan,
in consultation with relevant departments and agencies, to execute the
actions identified to secure 5G infrastructure and development. The
Implementation Plan will follow the four lines of effort identified in
the Strategy, laying out specific activities to achieve the goals of
the Strategy.

Request for Comment: Through this Request for Comments, NTIA is
seeking public input to inform the development of the Implementation
Plan. NTIA is looking for information as to how the U.S. Government can
best facilitate the accelerated development and rollout of 5G
infrastructure in the United States and with our international
partners, and lay the groundwork for innovation beyond 5G.
Specifically, NTIA is seeking feedback on the following questions,
organized by the four lines of effort laid out by the Strategy.

Questions

Line of Effort One: Facilitate Domestic 5G Rollout.

(1) How can the United States (U.S.) Government best facilitate the
domestic rollout of 5G technologies and the development of a robust
domestic 5G commercial ecosystem (e.g., equipment manufacturers, chip
manufacturers, software developers, cloud providers, system
integrators, network providers)?

(2) How can the U.S. Government best foster and promote the
research, development, testing, and evaluation of new technologies and
architectures?

(3) What steps can the U.S. Government take to further motivate the
domestic-based 5G commercial ecosystem to increase 5G research,
development, and testing?

(4) What areas of research and development should the U.S.
Government prioritize to achieve and maintain U.S. leadership in 5G?
How can the U.S. Government create an environment that encourages
private sector investment in 5G technologies and beyond? If possible,
identify specific goals that the U.S. Government should pursue as part
of its research, development, and testing strategy.

Line of Effort Two: Assess Risks to and Identify Core Security
Principles of 5G Infrastructure.

(1) What factors should the U.S. Government consider in the
development of core security principles for 5G infrastructure?

(2) What factors should the U.S. Government consider when evaluating the trustworthiness or potential security gaps in U.S. 5G infrastructure, including the 5G infrastructure supply chain? What are the gaps?

(3) What constitutes a useful and verifiable security control regime? What role should security requirements play, and what mechanisms can be used to ensure these security requirements are adopted?

(4) Are there stakeholder-driven approaches that the U.S. Government should consider to promote adoption of policies, requirements, guidelines, and procurement strategies necessary to establish secure, effective, and reliable 5G infrastructure?

(5) Is there a need for incentives to address security gaps in 5G infrastructure? If so, what types of incentives should the U.S. Government consider in addressing these gaps? Are there incentive models that have proven successful that could be applied to 5G infrastructure security?


(1) What opportunities does the deployment of 5G networks worldwide create for U.S. companies?

(2) How can the U.S. Government best address the economic and national security risks presented by the use of 5G worldwide?

(3) How should the U.S. Government best promote 5G vendor diversity and foster market competition?

(4) What incentives and other policy options may best close or narrow any security gaps and ensure the economic viability of the United States' domestic industrial base, including research and development in critical technologies and workforce development in 5G and beyond?

Line of Effort Four: Promote Responsible Global Development and Deployment of 5G.

(1) How can the U.S. Government best lead the responsible international development and deployment of 5G technology and promote the availability of secure and reliable equipment and services in the market?

(2) How can the U.S. Government best encourage and support U.S. private sector participation in standards development for 5G technologies?

(3) What tools or approaches could be used to mitigate risk from countries' 5G infrastructure? How should the U.S. Government measure success in this activity?

(4) Are there market or other incentives the U.S. Government should promote or foster to encourage international cooperation around secure and trusted 5G infrastructure deployment?

(5) Both the Department of Commerce and the Federal Communications Commission (FCC) have rulemakings underway to address the security of the telecommunications infrastructure supply chain. Are there other models that identify and manage risks that might be valuable to consider?

--------------------------------------------------


--------------------------------------------------

(6) What other actions should the U.S. Government take to fulfill the policy goals outlined in the Act and the Strategy?

[[Page 32018]]

Instructions for Commenters: This is a general solicitation of comments from the public. We invite comments on the full range of
questions presented by this RFC and on issues that are not specifically raised. Commenters are encouraged to address any or all of the questions above. Comments that contain references to specific court cases, studies, and/or research should include copies of the referenced materials along with the submitted comments. Commenters should include the name of the person or organization filing the comment, as well as a page number on each page of the submissions. All comments received are a part of the public record and will generally be posted on the NTIA website, https://www.ntia.gov/, without change. All personal identifying information (for example, name or address) voluntarily submitted by the commenter may be publicly accessible. Do not submit confidential business information or otherwise sensitive or protected information.

Kathy Smith,
Chief Counsel, National Telecommunications and Information Administration.
[FR Doc. 2020-11398 Filed 5-27-20; 8:45 am]
BILLING CODE 3510-60-P