GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

June 1, 2018

Dr. Charles Clancy
Director and Professor
Hume Center for National Security and Technology
Virginia Tech
900 North Glebe Road
Arlington, VA 22203

Dear Dr. Clancy:

Thank you for appearing before the Subcommittee on Communications and Technology on Wednesday, May 16, 2018, to testify at the hearing entitled "Telecommunications, Global Competitiveness, and National Security."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on Friday, June 15, 2018. Your responses should be mailed to Evan Viau, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed to Evan.Viau@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Marsha Blackburn
Chairman
Subcommittee on Communications and Technology

cc: The Honorable Michael F. Doyle, Ranking Member, Subcommittee on Communications and Technology

Attachment

Attachment—Additional Questions for the Record

The Honorable Pete Olson

1. Some might say that the U.S. is already "catching up" with other nations in the race to 5G. Whether or not that is an accurate assessment, there are many more nascent technologies that are still in the early stages of development, such as AI, autonomous vehicles, robotics, and bio-tech to name a few. How do we ensure that the U.S. remains a competitive force in these fields while also guarding against national security threats?

The Honorable Bill Johnson

1. Early analysis suggests that when it comes to quantum computing and quantum communications, the U.S. has shown interest in building the hardware, and China and Japan have been more focused on the applications, software, and use-cases. Global competition in the early stages of this race will shape the vendor landscape in future years when quantum communications may have commercial applications.

    a. What are the implications in the race to develop and deploy super- and quantum-computing capabilities and quantum communications on a wide scale?

    b. Will competitively developing our own systems position us to tackle threats to competition as the technology develops?

The Honorable Chris Collins

1. As we heard repeatedly in the testimony, threats not only arise with the equipment out of the box, but often with the long-term access to that equipment by offering ongoing servicing and upgrades. We've also heard that organizations – both the government and private companies – should take a risk management approach to ensuring the security of their networks. What steps can smaller, or rural, providers take to limit their vulnerability?

2. In your testimony, you discussed recent changes to the membership of standards bodies which set rules for equipment providers and suppliers. If one country or company sends a disproportionate number of representatives to a standards body, how does that impact the standards body's recommendations?

    a. Is it possible for nefarious actors use their participation in a standards body to influence the outcomes in order to create a competitive advantage for their company?

    b. With the power standards bodies have to shape the technical foundations of the networks and devices we use every day, how can we ensure that International

standards bodies determine standards based on the best technology, and not the loudest voices? For example, should there be greater transparency or mechanisms to standardize the representation of the members who contribute to these standards bodies?

The Honorable Mimi Walters

1. DHS, as the Sector Specific Agency for Telecom, is looking into both supply chain risks—including 5G and systemic risks more broadly. The FCC's CSRIC is also looking into supply chain risks related to 5G. The FCC CSRIC Report is due in September, and the DHS effort may conclude some time later before the end of the year. How do we avoid duplicative or potentially conflicting recommendations from all of these parallel efforts?

    a. Should we vest decision-making at one agency?

2. What level of sophistication does it take to exploit a vulnerability in the physical hardware of this equipment?

    a. How does that compare to the sophistication required to exploit the software components?

    b. Are either of these threats resolved solely by ripping and replacing vulnerable equipment?

    c. Is there a more thoughtful approach you could offer?