WILKINSON) BARKER) KNAUER) LLP

1800 M STREET, NW
SUITE 800N
WASHINGTON, DC 20036
TEL 202.783.4141
FAX 202.783.5851
WWW.WBKLAW.COM
CLETE D. JOHNSON
202.383.3405
CJOHNSON@WBKLAW.COM

June 15, 2018

Evan Viau
Legislative Clerk
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

Re: *Responses to Questions for the Record*

Dear Evan:

In response to Chairman Marsha Blackburn's request of June 1, 2018, please find attached my answers to the additional questions from Members of the Subcommittee on Communications and Technology following the hearing on May 16, 2018 entitled "Telecommunications, Global Competitiveness, and National Security."

It was an honor to testify at the hearing, and as noted in my attached answers to Members' questions, I would be happy to follow up on these important issues if they or their staff personnel have any further questions on which I may be of assistance.

Sincerely,

Clete D. Johnson

Responses to Questions for the Record

Clete D. Johnson
Partner, Wilkinson Barker Knauer LLP

Hearing on Telecommunications, Global Competitiveness, and National Security
May 16, 2018

House Committee on Energy and Commerce
Subcommittee on Communications and Technology

The Honorable Pete Olson

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?

Over the long term, boosting consumer and business confidence in the security of U.S. networks and their constituent equipment and services will play a crucial role in keeping the United States ahead of the competitive curve in all of these areas.

Secure, reliable networks built through trusted suppliers of equipment and services are the key to this future market leadership. The U.S. government and a broad collection of industry stakeholders have undertaken collaborative efforts toward innovation among trusted suppliers and a secure and vibrant internet and communications ecosystem through many policy and standards processes. For instance, initiatives led by the Departments of Commerce and Homeland Security under Executive Orders 13636 and 13800, along with international efforts such as the Common Criteria for Information Technology Security Evaluation, the Open Group Trusted Technology Forum, and the International Standards Organization, have provided avenues to advance both innovation and security.

As we develop methods to identify and promote competition among trusted suppliers, we must also identify suppliers whose corporate structures, personnel, and relationships with adversary governments and intelligence services are particularly susceptible to tactical or strategic exploitation. This is the focus of significant recent policy activity in the Executive Branch and in Congress. Going forward, the Department of Homeland Security (DHS), as the Sector Specific Agency for both the communications and the IT sectors, should coordinate these efforts through thorough interagency processes that take in pertinent information from expert government agencies such as the Departments of Defense, Commerce, and State, and the FBI and other appropriate elements of the law enforcement and intelligence communities. The actions of the Federal Communications Commission (FCC) and other regulatory authorities should also be coordinated within these broader processes. Additionally, to promote collaborative and candid

partnership with the industry stakeholders who know these markets best, sensitive private sector information provided to the government by individual companies should be formally protected under the Protected Critical Infrastructure Information Act, administered by DHS, which prohibits both public disclosure of protected information and use of such information in civil litigation or regulatory rulemaking or enforcement actions. Over the longer term, formal supply chain security determinations regarding which suppliers or particular equipment or services should be subject to special security scrutiny, restrictions or prohibitions should derive from these broader interagency processes or related statutory requirements.

The Honorable Bill Johnson

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?*

As discussed in the hearing, I believe that collaborative and multistakeholder efforts like those undertaken by the Department of Commerce – particularly the quantum computing work conducted by the scientists of the National Institute of Standards and Technology (NIST), along with leading academic and industry experts – can allow for transformative breakthroughs in security, computing, and communications. The key to harnessing the potential of these advances is for the U.S. government to use its convening authority, along with funding and other support for basic research, to allow U.S. innovators to flourish. In contrast, centrally-planned, top-down government industrial policy may be the approach of autocratic governments such as China's, but it is not the best approach for the United States to achieve the full potential of our uniquely innovative society.

The Honorable Chris Collins

As we've 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?

The challenge of supply chain security is perhaps most acute for smaller providers that operate with lower margins and less capital resources and staff than larger national providers.

As discussed in the hearing, the Federal Communications Commission (FCC) has begun a formal rulemaking process proposing to prohibit Universal Service Fund (USF) support for purchases of equipment and services from companies that pose a national security threat to the United States' communications infrastructure. This proposal cites three companies: Huawei, ZTE, and Kaspersky Lab. This notice-and-comment rulemaking process is producing the first-ever substantial and detailed public record on these issues. The 23 comments submitted in the first round of comments in this proceeding, submitted on June 1, collectively contain significant discussion of the market considerations pertaining to a possible prohibition of Huawei and ZTE from the USF-supported market; the reply round of comments, due July 2, is expected to further flesh out the record regarding this market.

While the rules that may result from this proceeding could ultimately disrupt the present supply chains of certain providers to some extent, the record that is developing through this notice-and-comment process may be particularly valuable in finding creative and cost-effective solutions to the challenges that confront small providers in particular. For instance, the newly intense focus on these supply chain security issues may illuminate new possibilities for further developing information sharing capabilities, government assistance partnerships, and collaborative relationships with larger peering partners beyond those that exist today. I would be happy to follow up with your staff in further detail following the completion of this record.

The Honorable Mimi Walters

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?

The Department of Homeland Security (DHS), as the Sector Specific Agency for both the communications and the IT sectors, should coordinate thorough interagency processes on supply chain security that take in pertinent information from expert government agencies such as the Departments of Defense, Commerce, and State, and the FBI and other appropriate elements of the law enforcement and intelligence communities. The actions of the Federal Communications Commission (FCC) and other regulatory authorities should also be coordinated within these broader processes. Additionally, to promote collaborative and candid partnership with the industry stakeholders who know these markets best, sensitive private sector information provided to the government by individual companies should be formally protected under the Protected Critical Infrastructure Information Act, administered by DHS, which prohibits both public disclosure of protected information and use of such information in civil litigation or regulatory

rulemaking or enforcement actions. Over the longer term, formal supply chain security determinations regarding which suppliers or particular equipment or services should be subject to special security scrutiny, restrictions or prohibitions should derive from these broader interagency processes or related statutory requirements.

The Honorable Anna G. Eshoo

1. *During my questioning, I asked if anyone had done an analysis on the trusted supply chain to determine whether it is viable for our country to eliminate our dependence on foreign adversarial companies like Huawei and ZTE. You told me it had not, but you would follow up.*

    a) *Have you or anyone begun to conduct such an assessment?*

    b) *If not, are you willing to do so?*

While I am not aware of a publicly available analysis that directly answers this question, there are multiple pertinent government-industry processes underway that may begin to provide the foundation for such an analysis.

First, the Federal Communications Commission (FCC) has begun a formal rulemaking process proposing to prohibit Universal Service Fund (USF) support for purchases of equipment and services from companies that pose a national security threat to the United States' communications infrastructure. The notice for this proposed rulemaking cites three companies: Huawei, ZTE, and Kaspersky Lab. This notice-and-comment rulemaking process is producing the first-ever substantial and detailed public record on these issues. The 23 comments submitted in the first round of comments in this proceeding, submitted on June 1, collectively contain significant discussion of the market considerations pertaining to a possible prohibition of Huawei and ZTE from the USF-supported market; the reply round of comments, due July 2, is expected to further flesh out the record regarding this market.

Also, the FCC has tasked its Communications Security, Reliability and Interoperability Council (CSRIC), a formal Federal Advisory Committee of private sector and other experts, to conduct a study to "identify and examine the security risks to the emerging 5th generation [5G] wireless networks." Among other tasks, the CSRIC has been asked to provide recommendations to address "vulnerable supply chains." The CSRIC report for this 5G-focused effort is due in September. While this effort is aimed primarily at developing "best practices for the design, deployment, and operation of risk-tolerant 5G networks to mitigate the identified risks," rather than a purely market-oriented analysis of specific suppliers, the public findings and recommendations in this report will augment the public record that will have been created through the separate FCC rulemaking process mentioned above.

Additionally, the Department of Homeland Security (DHS) has begun a program of Telecommunications Supply Chain Risk Assessments that will consist of both general assessments of the sector's supply chain risks and targeted assessments of specific threats, vulnerabilities and entities at risk. The general risk assessment is expected to be completed and published by August 31, and the targeted assessments will begin thereafter.

Meanwhile, the Commerce Department's National Institute of Standards and Technology (NIST) and National Telecommunications and Information Administration (NTIA) continue multiple workstreams, respectively, for developing supply chain risk management guidance and conducting policy analysis and multistakeholder consensus building for internet and communications ecosystem best practices.

All of these processes are advancing our understanding of these issues and will provide new publicly available information to augment other government, private sector, and academic studies of more discrete components of this market challenge. In particular, following the submission of reply comments in the FCC's rulemaking proceeding on July 2, there will likely be a public record sufficient to begin the market analysis that you are seeking. Of course, if you wish, I would be happy to explore further with your staff the available public resources for, and the possible parameters and methodologies of, such an analysis.

2. *Did you agree with the Department of Commerce's decision to implement a seven-year ban on ZTE?*

    a) *If so, should the Department and other U.S. officials investigate whether similar bans are appropriate for other Chinese entities, as Senator Rubio has suggested?*

    b) *Should the Administration continue to indulge ZTE and other companies in 'deals' when we know outright that the company has repeatedly undermined our laws?*

    c) *What is the potential for harm to our national security by having foreign adversaries involved in business with U.S. small businesses and start-ups?*

ZTE's scheme to evade U.S. export controls was an egregious violation of laws that protect our national security. The law enforcement actions pertaining to ZTE's illegal activities and its reported violations of the 2017 settlement agreement – including any additional penalties or subsequent settlement agreements that may be appropriate – should be treated purely as law enforcement actions, separate and distinct from policy decisions or policy-related negotiations.

Regarding additional prohibitions beyond the existing export denial order against ZTE, as you well know, there are certain existing statutory prohibitions against federal procurement of ZTE, Huawei, and Kaspersky Lab. Pending legislation in Congress would expand these prohibitions against ZTE and Huawei, and possibly include altogether new statutory prohibitions against three video equipment companies. Beyond these companies that have been the subject of

statutory bans and/or related legislative attention, the FCC and DHS processes mentioned above should seek to establish thoroughly well-coordinated interagency processes, led by DHS as the Sector Specific Agency for the communications and IT sectors, that take in relevant information from expert government agencies and private sector stakeholders to determine which if any other suppliers or particular equipment or services should be subject to special security scrutiny, restrictions or prohibitions. Over the longer term, any such action should derive directly from these broader interagency processes or statutory requirements.

Finally, regarding the question about foreign adversaries' targeting of small businesses and start-ups, this part of the market can be fertile ground for adversaries' infiltration and espionage. As you well know, the technological advances in Silicon Valley and other innovation hubs is one of the United States' greatest strategic assets. Adversaries' infiltration and/or theft of these companies' proprietary business processes and intellectual property is a serious strategic national security concern.

3. *What would be the costs to U.S. industry be to comply with laws that would prevent companies from using Huawei or ZTE equipment or equipment produced in China?*

    a) *What would be the costs to U.S. industry of replacing Huawei or ZTE equipment that may be on their networks?*

    b) *What would be the costs to U.S. industry of complying with laws that would prevent companies from using Huawei or ZTE equipment or equipment produced in China?*

    c) *What would be the costs to U.S. industry of complying with laws that would prevent companies from using Huawei or ZTE equipment or other equipment produced in China?*

As discussed above in Question 1, the multiple ongoing government-private sector processes will provide new publicly available information to address these cost/benefit questions. In particular, the FCC's rulemaking proceeding (reply comments due July 2) is creating the first substantial and detailed public record on these issues, and that record will provide a base of information from which to derive answers to these questions. As with the market analysis you requested at the hearing and in Question 1 above, I would be happy to develop answers to these questions with the benefit of the full record in the FCC proceeding, following the July 2 submission of reply comments.