Responses to *Questions for the Record*

Dr. Charles Clancy, Professor of Electrical and Computer Engineering, Virginia Tech

before the House Energy and Commerce Committee, Subcommittee on Communications and Technology, Hearing on Telecommunications, Global Competitiveness, and National Security

June 15, 2018

The following document provides responses to the questions for the record for the hearing entitled "Telecommunications, Global Competitiveness, and National Security" on *May 16, 2018.*

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 the US remains a competitive force in these fields while also guarding against national security threats?**

The US Government spends $140B per year on research and development (R&D), which is around 30% of total R&D investment in the US. These investments are crucial to helping the US remain competitive in the global innovation marketplace. While the US's R&D investment is increasing an average of 4.4% per year, China's investment is increasing at a rate of 16% per year, and is expected to overtake the US by 2020. Additionally in areas like bio-tech, China places fewer regulatory and ethical restrictions on research which affords them some unique advantages.

The US cannot out-spend China in R&D over the long term. Thus the US needs to be selective. Programs are needed to focus investments in areas critical to national security, such as those mentioned (AI, autonomy, bio-tech). Ordinarily this focused investment strategy would be overseen by the Office of Science and Technology Policy (OSTP) in concert with the major R&D investment departments and agencies; however, the lack of senior-level appointees and staff detailees makes it difficult for OSTP effectively execute this mission.

Recent White House coordination around Artificial Intelligence is a positive step forward. Similar efforts are needed in autonomy, quantum, and bio-tech. In all these areas a national strategy is needed that can help connect basic research funded by the National Science Foundation (NSF) and National Institutes of Health (NIH) to the applied research envisioned by the Department of Defense (DOD) and Intelligence Community (IC) to tackle key areas of national security.

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 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?**

Quantum computing and quantum communications are technologies that will revolutionize computing and telecommunications over the next 20 to 30 years. Indeed most federal R&D funding to date has focused on the physics of quantum computing, and recent legislation proposed within the Senate also seems oriented toward further investment in the underlying physics. At this point there is sufficient industry interest in the technology that we will see vendors like IBM and D-Wave make investments that will continue to increase the number of qubits offered by their systems. We are on the cusp of these systems' quantum speedups outpacing conventional computing and surpass Moore's Law.

Investment in applications is critical. If current legislative proposals around quantum research institutes are going to have a meaningful market impact, they must dedicate the majority of their resources into developing algorithms and applications that can leverage emerging quantum computing platforms, and let the promise of these applications drive continued industry investment into the device physics. The Quantum industry is still searching for and seeking to demonstrate the "killer app" that will drive continued investment in the technology.

Regardless of national security concerns, quantum computing is going to exist within a global marketplace. Therefore the US needs to begin investing now in quantum-resistant secure communications technologies. Current solutions like quantum key distribution address this challenge in very limited scenarios, and there needs to be added focus on application-layer public-key cryptography that can stand up to the capabilities of a quantum supercomputer.

<u>The Honorable Chris Collins</u>

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 the 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 rural providers take to limit their vulnerability?**

While one-size-fits-all compliance approaches can often be unaffordable to smaller operators, risk-based management approaches are inherently designed to scale with the size and resources of the organization, from the large multi-national company all the way down to the individual user. By evaluating risk, small, rural providers can identify the areas where investment in cyber defense can be most meaningful in combating the threat.

A key opportunity for rural providers is participation in emerging cyber threat information sharing communities. The FCC's Communications Security, Reliability and Interoperability Council (CSRIC) studied information sharing and released a report in March 2017 detailing ongoing programs and opportunities for further connectivity through sharing cyber threat information across industry. As these programs mature through venues such as the Telecommunications Information Sharing and Analysis Center (ISAC), the scale and capabilities of larger providers can be brought to bear to support smaller operators.

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 to use their participation in a standards body to influence the outcome in order to create a competitive advantage for their company? (b) With the power standards bodies have to shape the technical foundation of the network devices we use every day, how can we ensure the 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?**

Standards bodies are inherently designed for transparency, and their underlying business model presumes that participating organizations, whether companies or governments, are working to advance their own agendas. These agendas typically revolve around companies seeking to have their intellectual property written into the standards in order for them to garner long-term royalties. As Chinese companies seek to further establish themselves in the global tech economy, having their intellectual property included in standards is a key step. The drivers around this are more economic than seeking to advance a hidden agenda.

The biggest opportunity for the US to maintain a leadership role in standards is for the US Government to increase its role in the standardsmaking process. There has been a considerable decline in participation from organizations such as the National Institute for Standards and Technology (NIST) in standards bodies like the Third Generation Partnership Project (3GPP) and Internet Engineering Task Force (IETF). As foreign countries and companies increase their involvement in standards processes, the best check on that influence would be direct US government participation to help articulate clear priorities.

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 these parallel efforts? Should we vest decision-making authority at one agency?**

There is broad consensus from industry that one agency should take the lead and help coordinate interagency activities to reduce duplicative and potentially conflicting processes. As the Sector Specific Agency for telecommunications, DHS is the logical lead entity to address issues like this.

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?**

Exploiting vulnerabilities in devices requires discovery of the vulnerability, development of an exploit, and weaponizing that exploit. Generally speaking, it takes more sophistication and resources to discover vulnerabilities in hardware than software, and often discovering hardware vulnerabilities requires the resources of a nation state actor. Once discovered the sophistication needed to exploit the vulnerabilities is similar.

"Rip and replace" is certainly one approach to dealing with the issue, but represents one extreme on the risk management continuum. For highly-sensitive and/or nationally-critical systems, it may be the right choice.

However for device and systems of lower criticality or lower threat, a range of risk mitigation steps may be more appropriate. For example, in dealing with the potential threat of weaknesses in SS7, industry developed and deployed technology to monitor SS7 infrastructure for malicious use, and if detected use that information to block bad actors from accessing the infrastructure.