***Questions for the Record* Response for Dr. Charles Clancy**

**Bradley Professor of Cybersecurity, Virginia Tech**

**before the Senate Committee on the Judiciary, Hearing on 5G: The Impact on National Security, Intellectual Property, and Competition**

*June 4, 2019*

Given the consistent themes expressed across the Senators' questions for the record, my response below is an overall set of recommendations that address individual questions as part of the narrative, citing the specific questions that are included as an attachment.

**Topic Area 1: Understanding and addressing the intersections between telecommunications standards, intellectual property, and industrial competitiveness**

Within the standards process, individual contributors representing the interests of companies advance technical concepts that over time go from broad requirements and use cases, to high-level architectures, to detailed specifications. This process is messy, organic, and influenced by corporate interests. A key undercurrent through this process is Intellectual Property Rights (IPR) that may be associated with specifications being developed. As standards are developed, companies disclose IPR they believe applies to those specifications.

Upon completion of a specification, a list of standard essential patents (SEPs) is compiled. While the technologists authoring the patents are not intellectual property lawyers, and the applicability of certain SEPs can be challenged, the list of SEPs is broadly reflective of a consensus around what patents must be licensed by organizations that implement the associated technology. Standards Development Organizations (SDOs) require that SEPs be licensed under Fair, Reasonable, and Non-Discriminatory (FRAND) terms.

A 2014 study by Wilmer Hale found that as much as $150 of the cost of a cell phone can be royalties[1]. At 1.5 billion phones being shipped each year, this is a more than $200B in annual royalties. The more SEPs a company owns, the bigger their slice of this pie. Qualcomm generates a third of its revenue and the majority of its operating income from patent royalties. Patent disputes among major players often lead to multi-billion-dollar settlements and judgements.

In 2005, Huawei began ramping up its participation in SDOs. As an active participant at the time, I personally witnessed this shift. Huawei hired away some of the most productive standards contributors with lucrative bonus packages that rewarded contributors for each submission, with escalating payouts as submissions advanced through the standards process to being part of the final set of specifications. Huawei has used this same type of bounty program to incentivize IP theft[2].

Huawei's primary objectives in these engagements are economic. They seek to set the international standards such that their share of the royalties is higher. One such example is the debate over the type of error-correcting

[1] A. Armstrong, J. Mueller, T. Syrett, "The Smartphone Royalty Stack: Surveying Royalty Demands for the Components Within Modern Smartphones", Wilmer Hale Working Paper, May 2014, https://www.wilmerhale.com/-/media/ed1be41360634d1fa5c3ab08647e8ada.pdf

[2] USA v Huawei, "Theft of Trade Secrets Conspiracy," Indictment CR19-010, US District Court, Filed January 16, 2019, https://www.documentcloud.org/documents/5698470-Huawei-Indictment.html

codes used in 5G. Huawei has a significant patent estate in polar codes and fought to oust the US-led Low-Density Parity Check (LDPC) codes from 5G. Ultimately a compromise was reached where both are in different parts of the standard, which was a major win for Huawei in being able to monetize their IPR[3]. [Grassley QFR#1]

These standards and IPR fights are a tussle for economic superiority and influence, which has an indirect impact on national security. China is not putting back doors in the standard. They are not influencing SDOs to adopt inferior technology. They are steering standards in directions that net them royalty payments down the road. IPR revenue can then be invested back into R&D to further enhance their IPR position and economic dominance of the market. China's long-term market share can then be exploited to either directly or indirect enable espionage or cyber attacks for the PLA. [Booker QRF#3, Coons QFR#2, Tillis QFR#2, Grassley QFR#3, Grassley QFR#5]

The key question is then what we do about it.

First, you have to play to win. In 2018, of the standards submissions on 5G security[4], Huawei and its chipset subsidiary HiSilicon were responsible for 33%, Qualcomm 5%, and the US government (NIST and MITRE) 0.5%. Overall 59% of the submissions originated from China, 23% from Europe, and only 10% from the US.

To turn these trends around, we need to have a significant increase in presence, and that presence needs to yield active participation. One measure of active engagement is the number of standards contributions for each staff-day of participation. In 2018, within the 5G security standards, Huawei had 3.7 contributions per staff day of participation, Ericsson had 2.9, Qualcomm had 1.0, and USG had 0.3. These numbers demonstrate that Huawei is essentially flooding the SDOs with contributions, while US participants are much less active. The US needs more active participation from both industry and government. [Tillis QFR#1, Grassley QFR#3, Grassley QFR#5]

Accomplishing active industry participation is motivated financially by the opportunity for long-term royalty revenue. Given Huawei is out-spending Ericsson, Nokia, and Qualcomm combined in R&D, they have more raw material to work with.

There are a wide range of ways that USG can invest in R&D that would help advance active participation. These include [Tillis QFR#1, Grassley QFR#8]:

1. increase the federal R&D tax credit for qualified research in telecommunications (and potentially other areas of key national competition like AI and quantum);
2. increase the federal R&D tax credit for patent protection costs;
3. add participation in SDOs as a qualified activity for the federal R&D tax credit;
4. provide even larger incentives for new and small businesses in the federal R&D tax credit to motivate more SDO engagement by small companies;
5. provide funding supplements under the Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) programs for patent protection and SDO involvement; and
6. ensure incorporation of 5G topics in the SBIR and STTR programs for FY20 and beyond.

[3] I. Morris, "Huawei Has Billions Riding on Claim to Be 5G Patents Powerhouse", Light Reading, April 2019, https://www.lightreading.com/mobile/5g/huawei-has-billions-riding-on-claim-to-be-5g-patents-powerhouse/d/d-id/750587

[4] Statistics reflect submissions to 3GPP SA3 during calendar year 2018 during which there were a total of 3,582 contributions.

As a point of reference, current federal R&D tax credits reimburse 6% to 8% of research investments. For critical areas like telecom this should be increased to 15% and as high as 25% for new/small businesses. Recommendations for larger-scale R&D investment are proposed in the following sections as well.

**Topic Area 2: Securing global 5G infrastructure**

Securing global 5G infrastructure involves a multi-pronged approach: (1) reduce the global market share for less-trusted OEMs, particularly for the delivery of critical services and in doing so increase the market share of more-trusted OEMs, and (2) create best practices and technology solutions that will secure critical applications that traverse global telecom infrastructure with a heterogeneity of supplier and operator trust levels.

The first way to reduce less-trusted OEM market share is through national boycotts. US bans on Huawei and ZTE, and the US's efforts to have other countries adopt similar bans, represent a key example of this approach. However, in pursuing such boycotts, there need to be viable alternatives to banned products, with viability being both similar technical capabilities and similar costs associated with deployment. For example, the Wicker/Cotton/Warner *United States 5G Leadership Act of 2019* proposes $700M from future spectrum auction revenue to help smaller carriers offset the cost of deploying more expensive, non-Huawei equipment. The lack of financial resources in the EU and a larger existing Huawei install base has led to similar bans being financially infeasible in countries like Germany. [Grassley QFR#6]

The second way to reduce less-trusted OEM market share is to disrupt the supply chain of target companies leading to product delays and significantly increased costs. Last year the threatened sanctions against ZTE could have resulted in the company's bankruptcy, according to ZTE's CEO. The US has been flirting with this very large stick for quite some time, and in the meantime Huawei and others have begun stockpiling US chips and putting together plans to build future devices without US components. What would be a one-time hit to Chinese companies as they retool their supply chains and develop more indigenous capabilities (likely bailed out by the Chinese government) could be a significant, sustained hit to US companies if, for example, China closed its markets to Apple. The US needs to get the most possible value from the current impending sanctions in the ongoing trade dispute because regardless of whether the sanctions hold, Huawei and their peers will be retooling their supply chain to reduce dependence on US components. The only remaining question is whether Beijing implements catastrophic sanctions against US companies seeking to sell technology into the China market. [Booker QFR#4, Grassley QFR#6]

Regardless of the outcomes of ongoing boycotts and sanctions, Huawei and other Chinese companies will be part of the Internet backbone and its 5G infrastructure. As a result, we must design 5G applications with this in mind. While the density of Chinese equipment may be low in the US, it will likely be high in other parts of the world, and given the global interconnectedness of the Internet, cybersecurity challenges will persist. Even more-trusted vendors have occasional bugs in their code that can be exploited by hackers. This leads us to the need for a holistic risk management approach to telecommunications and the critical infrastructure segments that operate over it. [Booker QFR#4]

As the sector-specific agency for telecommunications, DHS CISA should continue with their plans to develop a comprehensive approach to security and supply chain risk management for telecom infrastructure. This should include resources for smaller carriers to become better informed about risk, best practices for securing the control and management planes of 5G infrastructure, and facilitating the establishment of cross-industry norms for less-trusted OEMs. Additionally, DHS CISA should work with smaller carriers who have existing Huawei equipment to mitigate risks, whether it be to replace equipment (should resources be available) or otherwise contained. [Booker QFR#1, Booker QFR#2]

Beyond just DHS, 5G applications like connected cars and smart grid require engagement from DOT, DOE, and other departments. 5G has the ability to establish virtual "network slices" that meet the unique service and security requirements of custom applications riding over the network. In some cases, these applications may not be contained wholly within the US and may require international interconnects. For example, DOD has expressed an interest in a "secure slice" available anywhere in the world.

To address this, a few specific things are suggested [Booker QFR#1]:

1. establish a policy that US carriers must use a trusted, US-based root of trust to secure their 5G roaming interconnects and core services;
2. make R&D investments in developing a multi-stakeholder National 5G Security Testbed, and use that testbed to prototype secure network slices for different critical infrastructure sectors;
3. via NIST's National Cybersecurity Center of Excellence, author best practices for secure network slices meeting the needs of specific 5G application areas; and
4. develop and implement policies and regulations through the appropriate sector-specific agencies that require and audit implementation of best practices for critical infrastructure sectors operating over 5G.

**Topic Area 3: National Initiative in Telecommunications**

Development of a generation of wireless technology takes approximately 15 years. The US has missed the window to compete for patents, IPR, and influence in standards for much of the core 5G functions. However, the window remains open for enhancements to 5G, or so-called "5.5G". Additionally, there is ample opportunity for the US to lead 6G if we act quickly.

The 6G development and deployment timeline is as follows:

- 2015-2025 – R&D and IP development
- 2022-2026 – requirements, use cases, industry consensus on broad strokes
- 2025-2030 – standards authorship
- 2027-2031 – product development
- 2028-2032 – commercial deployment

In order to be competitive, the US needs to make immediate investment into R&D. These investments will lead to US ownership of relevant patents for 6G, which will provide the basis for contributions to standards bodies. Additionally, this R&D can lead to startup companies that will commercialize the technology, ideally turning into direct competitors to Huawei over the next decade. If the US does not commit to making such an investment in the next year, China will.

In 2013, the EU invested €700M into the 5G Public Private Partnership (5GPPP) which attracted €3.5B in industry investment. The US must launch a similar effort, as the EU is not in a position to do so for 6G. Given the lack of an indigenous OEM ecosystem, the US investment needs to include a major R&D component that will lead to the invention and reduction to practice of the core enabling technologies of 6G.

Overall, $2B in investment is needed over the next decade, financed from auction proceeds for 5G and future 6G spectrum. The following are the proposed core aspects of the investment [Coons QFR#1, Coons QFR#2, Graham QFR#1, Grassley QFR#2, Grassley QFR#4, Grassley QFR#7]:

1. charter and resource NITRD as the overall coordinator of the "National Initiative in Advanced Telecommunications" ($2M/yr);
2. establish and resource a heterogeneity of NSF basic research programs, ranging from large centers to smaller grants from their CISE, ENG, and IIP directorates ($35M/yr);

3. establish and resource NSF educational programs (new curriculum, programs, degrees, and experiential learning) focused at building skills in the workforce for 5G research, development, implementation, deployment, and operations ($5M/yr);
4. establish and resource NIST programs for US universities and non-profit research laboratories to develop open-source reference implementations for 5G/6G components that could enable rapid technology development and integration, and provide more diverse supply chain options ($20M/yr);
5. establish and resource a heterogeneity of applied research programs across DHS, DOD, DOT, DOE, and DOC that invest in 6G systems, applications, security, and testing ($70M/yr);
6. task and resource FCC, NTIA, DOD, and DOS to develop a comprehensive strategy for 5G and 6G spectrum that leverages a heterogeneity of bands, both exclusive and shared approaches, and AI-fueled real-time coordination that can be advanced internationally through the ITU and WRC process ($3M/yr);
7. establish and resource a telecommunications standards engagement and coordination program within NIST that works across industry to represent a more integrated US position on standards across relevant SDOs, and lead the international effort in defining the requirements and use cases for 6G ($15M/yr); and
8. launch and resource a USG-backed venture capital fund similar to In-Q-Tel that invests in US-based telecommunications companies to provide capital to advance the reboot of the US telecom OEM industrial base ($50M/yr).

Note that many of these programs should have industry match requirements to promote investment of US R&D capital into development of advanced telecommunications technologies. These match requirements should start off small (e.g. 1:4) to promote capacity and coalition building, but should increase as the ecosystems mature (e.g. 2:1).

**Other Topics**

Question [Booker QFR#5] referenced the impact of the Sprint/T-Mobile merger on the 5G ecosystem. As a consultant supporting the FCC on the merger proceedings I must abstain from commenting.

**Conclusion**

While the consequences of falling behind in wireless technology are dire, it is not a hopeless situation. The US possesses certain technical advantages that could propel the US become to become the leader in Beyond-5G technologies. For example, the US is leading the way in spectrum sharing technologies (thanks to the DOD), enterprise cellular networks (private cellular networks not associated with a traditional service provider), cloud processing (the basic and fundamental change behind the 5G architecture), and in artificial intelligence and machine learning (what many consider will be the basis behind 6G). The US also possesses – bar none – the best universities in the world that attract the finest minds and can contribute to a unique ecosystem to participate in these next-gen large scale challenges. If enabled, universities can plan a significant role in the resurgence of the US wireless ecosystem for international leadership, with the help of DOD.

| Attachment | Questions for the Record |
|---|---|
| [Booker QFR#1] | The current 5G discussion is heavily focused on building a trusted 5G infrastructure, which is certainly necessary. However, there has been less focus on the task of guaranteeing that the apps and services utilizing the 5G networks are also secure, and on what steps we should take to ensure security is built in from the ground up and commensurate with the threats we face. A clean and truly secure 5G network should prevent malware from transporting across protected devices and prevent unauthorized command and control from exploited connected devices. The United States should continue to encourage architecture that guards against these threats and address lateral threat movement within the network. What actions should the Department of Homeland Security (DHS) take to ensure 5G networks will appropriately secure the applications and services riding on the networks— accounting for malware prevention and unauthorized command and control from exploited connected devices—not just the infrastructure of the networks themselves? |
| [Booker QFR#2] | In building a risk-based approach to supply-chain security, how should we gauge the threats around specific categories of equipment? For example, the 2019 National Defense Authorization Act (NDAA) included rules of construction addressing the interconnected nature of telecom networks and the fact that different components have varying abilities to route traffic or to read the underlying data they carry. |
| [Booker QFR#3] | Various panel members testified that the Chinese have been exerting political pressure and conducting block voting within standards-setting organizations like the European Telecom Standards Institute (ETSI), the International Telecommunication Union (ITU), the 3rd Generation Partnership Project (3GPP), and also at major telecommunications conferences. At the same time, Huawei's massive research and development budget has clearly contributed to their lead in 5G patent applications. According to one study, China's share of "standard essential patents" was at 34 percent, compared with 14 percent for the U.S. Indeed, Huawei alone is responsible for 15 percent of 5G patent applications.<br><br>Please explain how controlling the standards for a technology translates to controlling the market for that technology.<br><br>Which is a bigger problem for the United States when it comes to setting 5G standards – politically motivated voting patterns or the flood of foreign patent applications?<br><br>Can the United States effectively address the Chinese block-voting problem without committing substantially more resources to research and development and thereby increasing our volume of patent applications? |
| [Booker QFR#4] | Last week, the Trump Administration placed Huawei and approximately 70 of its affiliates on an "Entity List," meaning that U.S. suppliers may require a license to conduct business with Huawei's companies. Yesterday, May 20, in compliance with the President's orders, Google banned Huawei—the second-largest smartphone manufacturer in the world—from using anything but the open-source version of Android, cutting Huawei off from critical proprietary Google mobile services like Maps, Search, Play Store, Gmail, etc. If the ban were applied strictly, it could drive one of China's highest-profile companies out of business. However, late yesterday afternoon, the Commerce Department granted Huawei a 90-day reprieve from the import ban. This |

rapid succession of decisions and partial reversals has significant implications for national security, employment, and trade relations for the United States and China.

Qualcomm, a U.S. company, got two-thirds of its sales from China in its most recent fiscal year. Similarly, Intel, the largest U.S. maker of chips, got more than 60 percent of its sales from the Asia-Pacific region last year, with most of that coming through China and Taiwan. How will potential sanctions against Chinese companies affect U.S. companies like Qualcomm, Intel, Broadcom, and Xilinx that provide necessary components to Huawei equipment? How will China's recent commitment to spend more than $100 billion dollars for developing homegrown chip manufacturers affect the U.S. position?

What does it mean that Huawei, the second-largest smartphone manufacturer, will potentially be cut off from Google, the largest provider of mobile operating systems? Will the actions of this week be the catalyst that forces Huawei to develop its own mobile operating system? If so, how will that affect U.S. leverage in future potential standoffs?

Are the references to a tech "Cold War" overwrought? How could these situations escalate?

[Booker QFR#5] Many argue that consolidation in the telecommunications industry has made European—and not American—companies the leading Western manufacturers of the antennas, boxes, routers, switches, and beam-generating equipment that form the backbone of 5G technology. At the same time, U.S. regulators appear close to reaching a final decision on T-Mobile and Sprint's proposed merger. Proponents of the merger argue it could lead to more spending on infrastructure; however, carrier consolidation has historically posed problems for equipment manufacturers (i.e., as carriers consolidate the customer base for equipment, manufacturers sell less equipment).

Would the proposed merger between T-Mobile and Sprint be a good thing for non-Chinese equipment vendors?

Does consolidation in the telecommunications hardware supply chain constitute a vulnerability for the United States?

[Coons QFR#1] Tomorrow's 5G ecosystem is built upon a foundation of 5G research and development and standards setting that enable the entire wireless environment. The other elements—mobile phones and other wireless devices, 5G infrastructure, and mobile semiconductors—each present their own challenges and opportunities for U.S. leadership in 5G, and therefore U.S. national security. I understand that China and South Korea are outpacing the U.S. in securing patents on 5G technology, and that China is specifically promoting 5G as part of its ambitious "Made in China 2025" plan. How should Congress and the administration support U.S. companies engaged in foundational 5G R&D to ensure continued global leadership and protect national security?

[Coons QFR#2] Chinese companies are reportedly voting as a block within standards developing organizations for nationalistic purposes. Without U.S. leadership in 5G standards, foreign governments, including adversaries, may have unprecedented control over all aspects of the wireless ecosystem. How do standard-setting processes relate to national security, and how do we ensure that private standard development organizations are

adopting the best technology and affording fair treatment to innovative U.S. companies and inventors who develop core technologies related to 5G?

[Coons QFR#3] While our overseas competitors strengthen their position in 5G, we have been weakening our innovation ecosystem. Computer software patents are harder to obtain in the U.S. than in Europe or China, even though we want to incentivize technology like artificial intelligence and smart infrastructure. Thus, I am concerned that the current state of the law puts us at a critical disadvantage on the global stage. What policies should this Committee examine to ensure that innovative companies in the United States can compete in the 5G race?

[Graham QFR#1] We discussed security in the context of utilizing equipment from trusted vendors. However, there are only two companies working on the next generation foundational technology in the chipset market —Huawei and Qualcomm. What steps should be taken to ensure there are "trusted vendors" of the foundational technology for 6G?

[Grassley QFR#1] You mentioned in written your testimony how many of us are looking for a "smoking gun," or proof that a specific entity is acting on behalf of the Chinese Communist Party to influence our country. In fact, many actions by the Chinese government are not technically illegal. Developing and implementing new technology isn't against the law. Yet, while within the bounds of the law, these actions still present a national security threat.

How can we tell the difference between Chinese companies' espionage tactics from legitimate business decisions?

[Grassley QFR#2] You stated at the hearing that we should not focus only on how to protect our economic and national security interests from the already existing 5G networks, but that we must prepare ourselves for the future of 6G.

How can the United States Government address the issues of 6G development and deployment in a more effective and proactive way, while still confronting the current issues that 5G creates?

[Grassley QFR#3] Could you describe the key factors needed to ensure 5G standards are secure and robust? To what extent is there a federal role here?

[Grassley QFR#4] What additional steps could the federal government take to promote the development of 5G technology? To what extent could additional, targeted R&D investments increase the speed of 5G rollout?

[Grassley QFR#5] What are the potential risks of Huawei playing a role in developing 5G standards? How can these risks be mitigated?

[Grassley QFR#6] What considerations, if any, should federal regulators, like the Federal Trade Commission and the Department of Justice, take into account when protecting competition for companies developing 5G technology?

[Grassley QFR#7] What steps, if any, could federal agencies take to incentivize additional domestic market participants in the 5G technology space?

[Grassley QFR#8] What role does patent protection play in incentivizing the development of 5G technology?

[Tillis QFR#1] U.S. leadership in the underlying technologies that make up 5G is a matter of national security. The Committee on Foreign Investment in the United States recognized as much when it found that a "[r]eduction in Qualcomm's long-term technological competitiveness and influence in standard setting would significantly impact U.S. national security." U.S. supply chain security in wireless starts with the technology and standards that form the foundation of 5G. Without U.S. leadership in the underlying 5G standards, foreign governments and businesses, including adversaries, will have virtually unfettered control over all aspects of the 5G ecosystem. How does standard-setting processes relate to U.S. national security, and what steps should Congress take to ensure continued U.S. leadership in 5G standard-setting in the interest of national security?

[Tillis QFR #2] The development of a 5G ecosystem requires communications standards, which are a collection of technical specifications developed by various engineers around the globe that define the contours of the technology. Standards are set by standards development organizations (SDOs) and their members. Because leadership in wireless standards requires both a willingness to make high-risk, long-horizon investments in R&D, as well as engineering expertise in the highly complex field of wireless communications, a relatively small number of companies make major contributions to wireless standards. Within SDO, innovative companies that develop standardized technologies are far outnumbered by "implementers" who participate in the standard to help select, learn and ultimately deploy the evolving technology. This disparity can lead to business disputes over licensing fees, with implementers hoping to pay lower royalties to innovators for the use of their standard-essential patents, and innovators expecting a fair return that incentivizes their significant investments in R&D. How do we ensure that SDOs—which are private entities—are adopting the best technology and affording fair treatment to the innovative companies and inventors who develop core technologies like 5G?