Question#:	1
Topic:	Reduced Cost
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	The Honorable Lindsey O. Graham
Committee:	JUDICIARY (SENATE)

Question: There was significant discussion about Huawei offering low-cost equipment. How are they able to offer their equipment for such a reduced cost?

Response: Huawei can offer technologies at reduced cost due to the significant support they receive from the Chinese Government. Per annual reports and public records, Huawei receives hundreds of millions of dollars in grants, heavily subsidized land to build facilities, apartments and bonuses for top employees, and massive state loans to international customers with little to no interest to fund purchases of Huawei products. The significant support received from the Chinese governments allows Huawei to undercut competitors.

Question#:	2
Topic:	Executive Order I
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	The Honorable Lindsey O. Graham
Committee:	JUDICIARY (SENATE)

Question: Last week, President Donald Trump issued an executive order restricting the ability of U.S. firms to sell technology to Huawei. Some companies are claiming that they can still license 5G network technology to Huawei because export control laws do not cover patents, as they are public records and therefore not confidential technology. Is this your same view or are these patents covered by the executive order?

Response: The restriction on exports of technology to Huawei by U.S. firms was put in place through the listing of Huawei on the Entity List, maintained by the Commerce Department, Bureau of Industry and Security (BIS), rather than the Executive Order on Securing the Information and Communications Technology and Services Supply Chain, issued on May 15, 2019. DHS defers to the Commerce Department on the application of U.S. export controls to the export of patented technology to Huawei.

Question#:	3
Topic:	Secure Networks
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: The Department of Homeland Security is in a unique position to address potential national security threats of a 5G network developed and deployed by Chinese companies. Because of the deep connections that Huawei and ZTE have with the Chinese Communist Party, their involvement in the growth of the 5G network is troublesome. China uses "soft power" to strategically influence and undermine our country's democratic values. We've seen this through the proliferation of Confucius Institutes and the theft of intellectual property and sensitive research at American universities. Recently, the Justice Department charged a Chinese businessman with economic espionage through the theft of technology at G.E., a company which supplies critical products to the U.S. military.

How does the Department of Homeland Security plan to ensure that our devices, systems, and networks are secure?

Response: The Department of Homeland Security (DHS) is working with our government, industry, and international partners to help ensure our nation's 5G-related devices, systems, and networks will have the necessary security controls.

Currently, the DHS Cybersecurity and Infrastructure Security Agency (CISA) and DHS Science and Technology Directorate (S&T) are working together to identify, prioritize, and mitigate risks to the entire mobile ecosystem. We have ongoing and planned research and development (R&D) efforts to develop cost-effective capabilities to address emerging cyber risks, such as those associated with supply chain threats; firmware and software vulnerabilities; and network-based monitoring, tracking, exploitation, and denial of service threats.

With regard to the public safety and continuity community, CISA is working to ensure our evolving mobile networks effectively support national security and emergency preparedness/response requirements, such as next generation priority and emergency services.
Specifically, CISA and FEMA are working with the Federal Communications Commission (FCC) and other public and private partners to ensure that national, state, and local Wireless Emergency Alerts (WEAs) and next generation 911 and reverse 911 services are effectively protected to prevent false alerts and ensure geo-targeted, reliable alerting to the public, emergency managers, and critical infrastructure owners and operators.

Question#:	3
Topic:	Secure Networks
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

With regard to securing federal networks, CISA carries out many activities that protect of federal networks and data. Assessment services and capabilities assist agencies in minimizing the impact of cybersecurity risks through the prioritized protection of high value assets and implementation of critical cybersecurity best practices. CISA also directs action, as appropriate, to address known threats to and vulnerabilities in federal networks. The combination of these activities enables CISA to rapidly share information, whether it is in response to a supply chain threat or a previously unknown software vulnerability, thus helping federal agencies secure devices, systems, and networks.

CISA is conducting activities to: (1) assess 5G risks; (2) evolve 5G policy in partnership with the "Whole of Community;" (3) safely and securely build 5G capacity; and (4) work with our industry and international partners to evolve 5G standards that are fair and protect U.S. national interests.

DHS is working with our academic, industry, and government partners to appropriately collaborate and share market information on engineering and security protocols, so DHS can better understand of current and evolving (unmitigated and mitigated) vulnerabilities and their potential impact to government missions and services.

Through the expansion of 5G network defense tools and capabilities, CISA, along and with other government and industry partners, will help ensure that 5G related devices, systems, and networks have continuous cyber threat diagnostics and controls to help appropriately identify and defend against malicious cyber activity and mitigate emerging threats.

Question#:	4
Topic:	Intellectual Property Theft and Espionage
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	The Honorable Lindsey O. Graham
Committee:	JUDICIARY (SENATE)

Question: With China's propensity to engage in intellectual property theft and espionage, what steps is the U.S. Government taking to guard against foreign companies using their semiconductor and other products to infiltrate and steal U.S. national security and national interest information and products?

Response: To protect our sensitive data, we are working to implement Section 889 of the 2019 National Defense Authorization Act and recently established the Federal Acquisition Security Council. The Department of Homeland Security (DHS) is also assisting the Department of Commerce with implementation of the Executive Order on Securing the Information and Communication Technology and Services Supply Chain. This Executive Order gives the Secretary of Commerce the authority to ban transactions of information and communications technology (ICT), deemed to be of unacceptable national security risk. DHS is providing an assessment on ICT elements (hardware, software, and services) to help ensure implementation of the Executive Order is risk informed.

In addition, as part of an investigation under Section 301 of the Trade Act of 1974, USTR found that China engages in a range of unfair and harmful conduct, including direction or facilitation of the acquisition of U.S. companies and assets by Chinese firms to obtain cutting-edge technologies through technology transfer, and conducting and supporting theft from computer networks of U.S. companies to obtain IP. On the basis of the findings of the Section 301 investigation, duties have been placed on Chinese goods in order to obtain elimination of China’s harmful acts, policies, and practices.

Question#:	5
Topic:	Embedded Foreign Company Devices
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: How are we protecting against the purchase of U.S.-built information technology equipment that may use embedded foreign company devices that would then leave us open to security vulnerabilities?

Response: Supply chain risk management (SCRM) is a top priority for DHS. Effective SCRM requires a whole of government and industry approach, and DHS is uniquely situated to play a lead role in this process. DHS CISA launched the ICT Supply Chain Risk Management Task Force, as the federal focal point for industry to drive SCRM solutions. The Task Force includes participation from 20 members of the information technology sector, 20 members from the communications sector, and 20 representatives across federal departments and agencies. Specifically, the Task Force is looking at how to better share supply chain threat information, providing a more consistent framework for supply chain threat assessment, developing criteria and processes that would eventually enable the creation of qualified bidder or manufacturer lists, and recommendations to incentivize the purchase of ICT from original equipment manufacturers or authorized resellers. The recommendations from the Task Force will advance our understanding of where there is unacceptable risk in the supply chain and solutions to mitigate those risks.

Additionally, the Federal Acquisition Security Council, through its ability to recommend issuance by the Secretaries of Homeland Security and Defense and the Director of National Intelligence of exclusion and removal orders applicable across the federal enterprise, will play a critical role in avoiding the use of technologies that present significant supply chain security risks.

Question#:	6
Topic:	Working With Other Agencies
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: I'm conducting oversight into the stealing of information, trade secrets, and taxpayer funded research. I've written to multiple federal agencies, including the Justice Department, Department of Health and Human Services and its Inspector General, and recently the National Science Foundation and the Department of Defense. In these letters, I've requested information about the threats posed by foreign actors, especially the Chinese government, that are seeking to steal U.S. intellectual property by exploiting U.S. research institutions, and the steps each agency has taken to detect and deter that threat. I've also requested an explanation of the vetting processes in place regarding researchers involved in taxpayer-funded research, and the steps each agency has taken to ensure that vetting is appropriate.

How can the Department of Homeland Security work with other agencies, such as DOJ, FBI, HHS, and DOD, to make sure that publicly funded research is not stolen right under our noses?

Response: As foreign actors target publicly-funded research, DHS is working to mitigate the risks that these actors pose. This includes operational activities to detect and respond to cyber incidents; information sharing activities; and efforts to strengthen the cybersecurity and resilience of federal agencies and non-federal stakeholders.

DHS CISA's 24/7 situational awareness, analysis, and incident response center provides assistance, including network protection; indicator sharing; information sharing and collaboration; incident response; malware analysis; vulnerability coordination; cybersecurity assessments; exercises; and training.

CISA works closely with our private and public-sector partners to share information on Chinese malicious cyber activity broadly with relevant stakeholders. Of note, was a serious of webinars and products CISA shared in 2019 related to Chinese malicious cyber activity.

Question#:	7
Topic:	Protect Secrets, Property, Information, and Research
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: I held a hearing on non-traditional Chinese economic espionage last year as Chairman of the Senate Judiciary Committee. During this hearing, it became clear that universities and research institutions aren't fully aware of what foreign governments, including China, are doing. Unfortunately, the gravity of the threat seems to be expanding beyond universities to the business world.

Given the concern of 5G networks allowing for Chinese influence in the United States, how can we improve our awareness to best protect our trade secrets, intellectual property, sensitive information, and research from being exploited and stolen from American universities and businesses?

Response: DHS, through CISA, is leading analysis and stakeholder engagement for 5G security and resilience efforts. As the Sector Specific Agency for the information and communications sectors, CISA is working closely with industry partners to develop a 5G risk characterization and promote 5G risk management practices. CISA is also conducting risk analysis to support the implementation of the Executive Order on Securing the Information and Communications Technology (ICT) and Services Supply Chain. This analysis consists of performing criticality assessments on an identified and validated taxonomy of ICT elements (hardware, software, and services). Additionally, CISA is working with other DHS components on 5G research and development efforts for mobile security. CISA has also been conducting outreach to universities and colleges to raise awareness of potential risks and to disseminate mitigation measures.

Collectively, these efforts and others will help all organizations – including universities and businesses – best protect their sensitive information from being stolen due to malicious activity that exploits 5G networks.

Question#:	8
Topic:	Executive Order II
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: The Administration signed an executive order on May 15, the day after the Judiciary Committee hearing, prohibiting the "acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology" where such a "transaction involves any property in which any foreign country or a national thereof has any interest (including through an interest in a contract for the provision of the technology or service)."

Does the Department of Homeland Security support this Executive Order?

Will the Department of Homeland Security play a role in ensuring the implementation of this order? If so, how will your department implement the order, and how will it coordinate with other federal agencies to ensure that it will prevent threats to national security and economic stability in the United States?

How does this Executive Order impact our foreign allies?

Response: As part of implementing the Executive Order on Securing the Information and Communications Technology and Services Supply Chain, the DHS CISA is assessing the national security risks stemming from vulnerabilities in telecommunications entities, hardware, software, and services – including components enabling 5G communication. This builds off existing engagement with the information technology and communications sectors to assess elements (hardware, software, and services) across the supply chain. CISA will be completing this analysis by identifying and validating with industry and government partners a standardized taxonomy of these information and communications technology (ICT) elements. CISA will then perform criticality assessments on these ICT elements with appropriate stakeholder input.

Ultimately, this analysis will inform the Secretary of Commerce’s exercise of authorities under the Executive Order.

Question#:	9
Topic:	5G Standards
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: Could you describe the key factors needed to ensure 5G standards are secure and robust? To what extent is there a federal role here?

Response: To ensure secure 5G standards, the United States continues to promote international standards and processes that are open, transparent, and consensus-driven and that do not place trusted companies at a disadvantage. The International Telecommunication Union (ITU) and the Third Generation Partnership Project (3GPP) both have U.S. companies as members, and one of the ITU's five top elected officials (the Director of ITU's Telecommunication Development Bureau) is currently a U.S. citzen. Members of the two groups representing U.S. suppliers' interests can promote standards that are currently being adopted and collaborate on their development. The United States is also working to achieve greater participation in the ITU, 3GPP, and other standard organizations.

Question#:	10
Topic:	5G Development
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: 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?

Response: The Federal government can encourage and invest in next generation communication technologies, which will likely position the United States to be a leading player in their rollout, potentially decreasing the influence of adversarial nations and decreasing U.S. reliance on untrusted technologies. The United States can begin to develop the next generations of communications technologies, whether wholly new technologies or advancements that improve upon 5G as a bridge to the next large advancement. Such development will occur in individual companies and in standards bodies, as markets for new services take shape.

Question#:	11
Topic:	Huawei 5G Role
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: What are the potential risks of Huawei playing a role in developing 5G standards? How can these risks be mitigated?

Response: Foreign nationals representing foreign companies, including Chinese companies China Mobile Communications Corporation and Huawei, hold key leadership positions on the ITU and 3GPP standards bodies for 5G. These individuals may be able to influence ITU and 3GPP to adopt standards that favor their own companies and put U.S. companies at a competitive disadvantage, potentially affecting their ability to compete in the market for years and increasing the United States' reliance on foreign technology. Therefore, additional engagement with international standards organizations by U.S. companies and the U.S. government can further mitigate risk. There are additional costs for organizations to be more engaged in international standards coordination, but supplemental funds might not be easily available

Question#:	12
Topic:	Domestic 5G Participants
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: What steps, if any, could federal agencies take to incentivize additional domestic market participants in the 5G technology space?

Response: The United States can incentivize domestic market participants by investing in national research and development, providing economic incentives for manufacturing in the U.S., buying trusted components, or implementing economic deterrents for purchasing and installing components designed and manufactured by companies with ties to or that could be compelled by foreign adversaries. This could increase trusted production and lower the risks of malicious Chinese technologies being inserted within the 5G technology space.

Question#:	13
Topic:	Starved of R&D Dollars
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	The Honorable John Cornyn
Committee:	JUDICIARY (SENATE)

Question: The U.S. has a vested national security interest in seeing developers continue to lead in all areas of the 5G race. I am particularly concerned about Chinese equipment manufacturers refusal to pay proper licensing standards for IP developed in the U.S. When Chinese companies do not pay proper licensing fees, the money stays inside the company providing billions in additional dollars for Chinese companies to invest in standards technology; while starving the US developers of the money that would be using for additional R&D in the standards space. Even more concerning, this problem is not just limited to the race for 5G. If we do not fix this disparity, it is impossible to expect U.S. innovators to continue developing at the same pace at the Chinese.

How can American companies compete in the development of 5G, 6G, AI, autonomous vehicle standards, and in all other sectors of the future, when US developers are intentionally being starved of R&D dollars by Chinese companies?

Response: American companies can continue to compete in the development of emerging technologies by participating in interoperability efforts, which will allow American companies to more easily incorporate new technologies within existing networks. Conversely, Chinese companies may be less likely to participate in interoperability efforts, potentially making it difficult for American companies to compete if Chinese companies have major market share.

The Federal Government can continue to take action to support American companies, by limiting the adoption of Chinese 5G equipment that may contain vulnerabilities. Section 889 of the 2019 NDAA prohibits federal agencies from procuring certain Huawei and ZTE equipment and services, and the recently enacted Federal Acquisition Supply Chain Security Act provides the government with important new authorities to address risks presented by the purchase of technologies developed or supplied by entities whose manufacturing and development processes, obligations to foreign governments, and other factors raise supply chain risks. The United States can also promulgate and promote technical best practices for mitigating aspects of 5G risk to support the development of emerging technologies.

Question#:	14
Topic:	IP Compliance
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	The Honorable John Cornyn
Committee:	JUDICIARY (SENATE)

Question: Should the USG consider forcing IP compliance by denying Chinese companies access to the U.S. market, until they are properly licensed?

Response: The U.S. Government should use a comprehensive strategic approach to address these issues.

U.S. Government actions against specific foreign threats, especially those that affect sectors like telecommunications and information technology, must remain well-coordinated to avoid unintended consequences for U.S. industry or broader U.S. Government interests.

Question#:	15
Topic:	CIFUS Review
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	The Honorable John Cornyn
Committee:	JUDICIARY (SENATE)

Question: Last year, I was proud to author legislation that helped close the gap on one of the existing tools used by the Chinese to acquire sensitive U.S. technology. My legislation, the Foreign Investment Risk Review Modernization Act (FIRRMA), strengthened the process whereby the Committee on Foreign Investment in the United States' vets' foreign investments in U.S. companies.

Given both DHS' and State's membership on the CFIUS Committee, are you both aware that Treasury's pilot program calls for transactions involving critical technologies in the fields of: wireless communications manufacturing, including semiconductor manufacturing and telephone apparatus manufacturing to be reviewed moving forward?

Do you believe that transactions involving these critical technologies should be highly scrutinized moving forward in order to protect the interests of U.S. national security?

Response: Our role as the leader of cutting-edge technology development is essential for sustaining our long-term primacy in information technology and economic growth. Scrutiny of transactions that involve the critical technologies detailed by FIRRMA is necessary in order to safeguard our national security interests.

Access to critical technologies, either by theft or the acquisition of US businesses and their intellectual property (IP), is key to China’s relentless pursuit to undermine our technological leadership position. Acquisitions of US businesses and their respective intellectual property in areas of critical technologies could raise national security concerns and pose a direct challenge to our economic, military, and technological primacy.

Question#:	16
Topic:	Escalating Tensions
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	The Honorable John Cornyn
Committee:	JUDICIARY (SENATE)

Question: As the United States and China continue to escalate economic tensions and begin to decouple supply chains, what is the effect on the competitiveness of companies who are looking to conduct research in this space?

Response: It's important that we continue to promote innovation and principles of vendor diversity, interoperability, and price transparency for all aspects of the ICT supply chain. By supporting and promoting the international recognition of the Prague Proposals, DHS is working to drive international consensus around the need for trusted ICT components. Additionally, DHS is conducting research and development activities by seeking development of new standards to improve the security and resilience of critical mobile communications networks. Specifically, we are examining innovative approaches and technologies to protect legacy, current and 5G mobile network communications, services and equipment against all threats and vulnerabilities.

All these efforts, and others, are critical to ensuring the competitiveness of trusted players in the ICT ecosystem.

Question#:	17
Topic:	Rural Markets
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	The Honorable Ben Sasse
Committee:	JUDICIARY (SENATE)

Question: Can you explain the extent to which rural telecommunications companies currently rely on Chinese technology to provide service in low coverage areas?

In a typical rural market, how large is the price differential between Chinese technology and the next cheapest supplier?

How do you expect these rural providers to be affected by listing Huawei on the Commerce Entity List?

Response: While a precise figure is not available, Chinese companies' aggressive focus on competitive pricing in underserved regions has enabled their global expansion despite ongoing security concerns. In the U.S., up to 25% of rural wireless carriers use Huawei equipment according to a Rural Wireless Association disclosure in an FCC filing.[1]

[1] FCC Filing: https://ecfsapi.fcc.gov/file/12080817518045/FY%202019%20NDAA%20Reply%20Comments%20-%20FINAL.pdf, p. 14

Question#:	18
Topic:	Alternative Hardware Suppliers
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	The Honorable Ben Sasse
Committee:	JUDICIARY (SENATE)

Question: How can we ensure over the medium- to long-term that alternative hardware suppliers not compromised by the Chinese are available?

Response: The Federal Government can ensure secure hardware suppliers are available by encouraging continued development of 5G technologies, services, and products. Reliance on Chinese 5G technologies is supported by relatively low costs. If Chinese companies' equipment is already installed as part of the 4G network, lack of interoperability may make it difficult to install other companies' 5G equipment without replacing the existing 4G equipment, which may be extremely costly.

Question#:	19
Topic:	Next Generation Technology
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	The Honorable Ben Sasse
Committee:	JUDICIARY (SENATE)

Question: What steps are we taking to prepare for the next generation of technology after 5G? Are we making any tradeoffs by focusing resources on the 5G problem now?

Response: 5G is the next generation of wireless communications technology. Combining new and legacy technology, 5G will build upon previous generations of wireless communications technology, in an evolution that will occur over many years. As future wireless communication technologies build off 5G technologies, the resources we are applying to 5G will shape future generations of wireless technologies. U.S. companies are continuing to pursue technical innovation to allow them to compete within the current 4G and 5G national and international wireless ecosystem, while at the same time conducting research to allow them to shape the future wireless and wireline communications infrastructures. The standards for 5G are maturing, which are allowing for initial deployments and testing.

Question#:	1
Topic:	Wireless Innovation
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	The Honorable Christopher Coons
Committee:	JUDICIARY (SENATE)

Question: 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. What is the administration doing to protect national security and ensure that the U.S. remains the leader in the innovation that underpins wireless technology? How can Congress help the administration in this effort?

Response: On May 15, 2019, the President issued an Executive Order (EO) on Securing the Information and Communications Technology and Services Supply Chain. The EO addresses the threat posed by the unrestricted acquisition or use of information and communications technology (ICT) and services from certain foreign suppliers. The EO prohibits certain transactions involving ICT and services, where the Secretary of Commerce, in consultation with leaders of other agencies, has determined that specified criteria are met, including that the transaction A) poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of information and communications technology or services in the United States; B) poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the digital economy of the United States; or C) otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons.

Through the EO, the Secretary of Commerce, in consultation with, or upon referral from heads of other agencies, can take various actions, including directing the timing and manner of the cessation of transactions prohibited pursuant to the EO, adopting appropriate rules and regulations, and employing all other powers granted to the President by the International Emergency Economic Powers Act, as may be necessary to implement the EO.

In addition, the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) has produced a risk assessment that "assesses and identifies entities, hardware, software, and services that present vulnerabilities in the U.S. and pose the greatest potential consequences to national security." The assessment "shall include an evaluation of hardware, software, or services relied upon by multiple

Question#:	1
Topic:	Wireless Innovation
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	The Honorable Christopher Coons
Committee:	JUDICIARY (SENATE)

information and communications technology or service providers, including the communications services relied upon by critical infrastructure entities identified pursuant to section 9 of Executive Order 13636."

CISA is coordinating with federal and private-sector partners to assess what hardware, software, and services present the greatest vulnerabilities in U.S. infrastructure and pose the greatest consequences to our national security.

In addition, as part of an investigation under Section 301 of the Trade Act of 1974, USTR found that China engages in a range of unfair and harmful conduct, including direction or facilitation of the acquisition of U.S. companies and assets by Chinese firms to obtain cutting-edge technologies through technology transfer, and conducting and supporting theft from computer networks of U.S. companies to obtain IP. On the basis of the findings of the Section 301 investigation, duties have been placed on Chinese goods in order to obtain elimination of China's harmful acts, policies, and practices.

Question#:	2
Topic:	Standard-Setting Process I
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	The Honorable Christopher Coons
Committee:	JUDICIARY (SENATE)

Question: 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 what steps is the administration taking to ensure U.S. leadership in 5G standard setting? How can Congress help the administration in this effort?

Response: 5G standard development may impact national security if standards are developed in a way that puts U.S. companies at a disadvantage. In standards organizations like 3rd Generation Partnership Project (3GPP), Chinese companies have submitted the greatest number of contributions. However, the 3GPP processes ensure that contributions are reviewed by consensus and are not automatically accepted. Contributions do not automatically become part of a specification, and the ones that do must receive support by other members to advance. They go through a rigorous deliberative and technical consensus process.

The addition of Huawei to the Export Administration Regulations (EAR) Entity List will likely hamper Huawei's efforts to gain and maintain supremacy in the 5G marketplace, as the planned roll-outs are now based on uncertain timelines and supply chains. Huawei's "polar code" (short code programming) and Qualcomm's competing LDPG (long code programming) were approved at the 5G standard setting conference 3GPPRAN on November 16, 2018. Qualcomm is likely in a favorable position to gain market share and drive standardization with LDPG if Huawei does not deploy its networks and technologies as planned.

Congress can continue to promote international standards and processes that are open, transparent, and consensus-driven and that do not place U.S. companies at a disadvantage. To ensure secure and robust 5G standards, United States companies who are eligible to participate could also work at achieving greater representation in the ITU, 3GPP, and other standard organizations.

Question#:	3
Topic:	Intellectual Property Protections
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	The Honorable Christopher Coons
Committee:	JUDICIARY (SENATE)

Question: A strong patent system is a necessity for U.S. inventors engaged in transformational research and development on 5G and beyond. What steps should Congress take to strengthen our intellectual property protections and incentivize continued U.S. leadership in 5G and other next-generation technologies?

Response: The U.S. Government can continue to promote international standards and processes that are open, transparent, and consensus-driven and that do not place U.S. companies at a disadvantage, particularly regarding intellectual property protections. To ensure secure and robust 5G standards, the United States could also work at achieving greater transparency and openness in the ITU, 3GPP, and other standard organizations.

Question#:	4
Topic:	Standard-Setting Process II
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	Senator Thom Tillis
Committee:	JUDICIARY (SENATE)

Question: 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?

Response: 5G standard development may impact national security if standards are developed in a way that puts U.S. companies at a disadvantage. In standard organizations like 3rd Generation Partnership Project (3GPP), Chinese companies have submitted the greatest number of contributions. However, the 3GPP processes ensure that contributions are reviewed by consensus and are not automatically accepted. Contributions do not automatically become part of a specification, and the ones that do must receive support by other members to advance. They go through a rigorous deliberative and technical consensus process.

The U.S. Government can continue to promote international standards and processes that are open, transparent, and consensus-driven and that do not place U.S. companies at a disadvantage. To ensure secure and robust 5G standards, the United States could also work at achieving greater representation in the ITU, 3GPP, and other standard organizations.

Question#:	5
Topic:	Fair Treatment
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	Senator Thom Tillis
Committee:	JUDICIARY (SENATE)

Question: 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?

Response: Committee chairs have a large influence over the contribution items that get considered in 3GPP. United States participants, including corporate, academic, government and the Alliance for Telecommunications Solutions (ATIS), should advocate for balanced representation at the leadership levels of 3GPP to ensure all parties are treated more fairly and have an opportunity to express their viewpoints. Other standards bodies may have different governance structures and not be subject to these concerns, for example if there are country voting representatives.

Question#:	6
Topic:	Secure 5G Networks
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	The Honorable Cory A. Booker
Committee:	JUDICIARY (SENATE)

Question: 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?

Response: DHS CISA and our federal partners can coordinate with industry partners to develop security capabilities that protect not only 5G infrastructure, but also the applications and services that utilize it. We can do this by incorporating a prevention-focused approach that focuses on visibility and security across the mobile network. Secure 5G applications and services will reduce the risk of malware infecting protected devices and unauthorized command and control exploiting connected devices. Together with our industry partners, CISA can also assisting with guarding against these risks within the 5G network.

Question#:	7
Topic:	Threats
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	The Honorable Cory A. Booker
Committee:	JUDICIARY (SENATE)

Question: 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.

Response: On May 15, 2019, the President issued an Executive Order (EO) on Securing the Information and Communications Technology and Services Supply Chain. The EO addresses the threat posed by the unrestricted acquisition or use of information and communications technology (ICT) and services from certain foreign suppliers.

The EO requires DHS CISA to produce a risk assessment that "assesses and identifies entities, hardware, software, and services that present vulnerabilities in the U.S. and pose the greatest potential consequences to national security." The assessment "shall include an evaluation of hardware, software, or services relied upon by multiple information and communications technology or service providers, I ncluding the communications services relied upon by critical infrastructure entities identified pursuant to section 9 of Executive Order 13636."

CISA is coordinating with federal and private sector partners to assess what hardware, software, and services present the greatest vulnerabilities in U.S. infrastructure and pose the greatest consequences to our national security.

Question#:	8
Topic:	Controlling the Standards
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	The Honorable Cory A. Booker
Committee:	JUDICIARY (SENATE)

Question: 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.

Please explain how controlling the standards for a technology translates to controlling the market for that technology.

Response: 5G standard development may impact national security if standards are developed in a way that puts U.S. companies at a disadvantage. In standard organizations like 3rd Generation Partnership Project (3GPP), Chinese companies have submitted the greatest number of contributions. However, the 3GPP processes ensure that contributions are reviewed by consensus and are not automatically accepted. Contributions do not automatically become part of a specification, and the ones that do must receive support by other members to advance. They go through a rigorous deliberative and technical consensus process.

The U.S. Government can continue to promote international standards and processes that are open, transparent, and consensus-driven and that do not place U.S. companies at a disadvantage. To ensure secure and robust 5G standards, the United States could also work at achieving greater representation in the ITU, 3GPP, and other standard organizations.

Question#:	9
Topic:	United States Response
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	The Honorable Cory A. Booker
Committee:	JUDICIARY (SENATE)

Question: 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?

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?

Response: The 3GPP standards organization is contribution-driven and meeting attendance is the best way to ensure a contribution is included in the standard. Patents, and research and development are integral to development of contributions. One way to increase U.S. standards involvement is to create academic programs involving 5G research and development that includes participation in the standards process.

5G standard development may impact national security if standards are developed in a way that puts U.S. companies at a disadvantage. In standard organizations like 3rd Generation Partnership Project (3GPP), Chinese companies have submitted the greatest number of contributions. However, the 3GPP processes ensure that contributions are reviewed by consensus and are not automatically accepted. Contributions do not automatically become part of a specification, and the ones that do must receive support by other members to advance. They go through a rigorous deliberative and technical consensus process.

The U.S. Government can continue to promote international standards and processes that are open, transparent, and consensus-driven and that do not place U.S. companies at a disadvantage. To ensure secure and robust 5G standards, the United States could also work at achieving greater representation in the ITU, 3GPP, and other standard organizations.

Question#:	10
Topic:	Potential Sanctions
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	The Honorable Cory A. Booker
Committee:	JUDICIARY (SENATE)

Question: 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?

Response: U.S companies that provide components to Huawei will be impacted by the addition of Huawei to the Entity List. The addition of Huawei technologies Co., Ltd. to the EAR Entity List on May 21, 2019, restricts all exports of EAR-controlled items to Huawei and its 68 affiliates in 26 countries without an individual export license. The impacts of this listing affect companies that supply specific technologies (i.e. semiconductors, smartphone chips, telecommunications network components) to Huawei.

Huawei's addition to the Entity List will likely hamper their efforts to gain and maintain market share in 5G, as the planned roll-outs are now based on uncertain timelines and supply chains. Huawei's "polar code" (short code programming) and Qualcomm's competing LDPG (long code programming) were approved at the 5G standard setting conference 3GPPRAN on November 16, 2018. Qualcomm is likely in a favorable position to gain market share and drive standardization with LDPG if Huawei does not deploy its networks and technologies as planned.

Question#:	11
Topic:	Huawei Mobile Operating System
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	The Honorable Cory A. Booker
Committee:	JUDICIARY (SENATE)

Question: 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?

Response: Google's Android operating system is used on Huawei smartphones. CISA understands that Huawei handsets will not be able to receive operating system updates unless Google obtains an export license if the ban is maintained. This imposes additional burdens on Huawei and could cause the company to look to another international, non-U.S. software company or find a domestic substitute. Huawei has publicly claimed it will develop its own operating system for its devices. This export ban illustrates Huawei's dependency on U.S. operating systems developers (Alphabet's Google Inc) and smartphone chip manufacturers. These chips are crucial to current smartphone manufacturing as they enable high performance front end transmit and receive solutions, facilitating the use of 5G technology.

Due to a reported stockpiling of some of these chips, CISA understands that Huawei may be able to manufacture phones for a yet undetermined amount of time.

Question#:	12
Topic:	Tech Cold War
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	The Honorable Cory A. Booker
Committee:	JUDICIARY (SENATE)

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

Response: 5G technologies will transform how we connect to the internet and introduce new risks. Which countries lead development of 5G technologies will affect security and innovation in an increasingly competitive environment. Decisions made today about 5G will affect national security and economic security for decades.

This is not only a competition among companies, but also between market-based and state-directed decision making. The United States has relied on the former, and China, for instance, on the latter.

The U.S. can manage 5G risk using two sets of policies. The first is to ensure that American companies continue to innovate and produce advanced technologies and face fair competition overseas. The second is working with like-minded nations to develop a common approach to 5G security. The United States cannot meet the 5G challenge on its own.

Question#:	13
Topic:	Consolidation
Hearing:	5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation
Primary:	The Honorable Cory A. Booker
Committee:	JUDICIARY (SENATE)

Question: 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?

Response: All the major U.S. carriers have already publicly committed to not using Chinese equipment in their deployment of 5G networks. From a national security standpoint a diversity of suppliers is not an inherent benefit though it can provide for greater security through both diversity and market competition for high quality and more reliable equipment. A single source supplier however - especially one who not only provides the equipment but also the operational construction, maintenance and management of a system – could be considered a high risk.