Prepared Testimony of
Commissioner Michael Wessel
before the
Senate Commerce, Science & Transportation Committee
February 6, 2019

Chairman Wicker, Ranking Member Cantwell, Members of the Committee. I want to thank you for the invitation to appear before you today to discuss the development and deployment of fifth generation—5G—cellular mobile communications. This is a critical issue for U.S. economic and national security interests.

My name is Michael Wessel and I am appearing before you today as a Commissioner on the U.S.-China Economic and Security Review Commission (Commission), where I have served since its creation in 2001. But, as a disclaimer, I am speaking for myself, although my comments are informed by my service on the Commission and our work on this issue.

The Commission was created by Congress in 2001 in conjunction with the debate about the grant of Permanent Normal Trade Relations (PNTR) to China, paving the way for its accession to the World Trade Organization. The Commission was tasked with monitoring, investigating and submitting to Congress an annual report on the national security implications of the bilateral trade and economic relationship between the United States and the People's Republic of China, and to provide recommendations, where appropriate, to Congress for legislative and administrative action.

The grant of PNTR ended the annual debate about whether to extend most favored nation status to China. But as it passed PNTR, Congress created the Commission because it did not want to forego the annual review of our relationship with China. Since the creation of the Commission, our mandate has been extended and altered as the U.S.-China relationship evolved.

The Commission is a somewhat unique body: We report to and support Congress. Each of the four Congressional leaders appoint 3 members to the Commission for 2-year terms. In 8 of the last 11 years, we have issued unanimous reports. In the 3 years where it was not unanimous, there was only one dissenting vote. In many ways, the evolving challenges and opportunities posed by the relationship with China have united us in our analysis.

Last year the Commission held a hearing on Next Generation Connectivity looking at both 5th generation (5G) connectivity and the Internet of Things (IoT) and included a chapter in our annual report on these issues. The prepared testimony and transcript of our hearing, as well as our Annual Report, are available online at the Commission's website www.uscc.gov.

The Commission has been tracking and analyzing China's high-tech development—and its impacts on the United States—for many years and found remarkable continuity and coordination

in Chinese government policy. Indeed, in the Commission's 2004 report, the key findings with regard to high technology were:

- The Chinese government has a coordinated, sustainable vision for science and technology development. Many Chinese high-technology developments have been spurred by policies the Chinese government has instituted to accelerate the growth of industries in this sector, which the government believes can help lift the whole economy.
- The Chinese government uses foreign investment, tax policies, subsidies, technology standards, and industry regulation to accelerate the nation's technological growth. It uses government procurement and proprietary technology standards to advance its technology growth policies. These policies make it difficult, if not impossible, to achieve a level playing field in this area of U.S.- China trade.
- Global production networks dominate China's high-tech export environment. Foreign investment into China has provided capital, management, and technology to Chinese production in various technology sectors. Taiwan firms are key investors and intermediaries in China's high-tech production networks.
- U.S. trade and investment with China has played, and continues to play, a key role in China's technological advancement. U.S. advanced technology and technological expertise is transferred to China, through both legal and illegal means, via U.S. invested firms and research centers in China, Chinese investments in the United States, bilateral science and technology (S&T) cooperative programs, and the tens of thousands of Chinese students and researchers at U.S. universities and research institutes who return to China after completing these programs.
- Large-scale piracy—at levels of over ninety percent—continues to characterize intellectual property rights (IPR) protection in China and is a major concern for U.S. exporters of high-tech goods and services. While the government has instituted laws to strengthen IPR protection, the enforcement of those laws has suffered from a lack of government coordination and from local protectionism and corruption.

In our report the following year, the Commission noted 3G—a precursor to the technology which is the subject of today's hearing—was identified by China's government as a key interest:

- China has its own globally approved 3G standard, TD–SCDMA for use in mobile telecommunications. It was developed by the Chinese Academy of Technology and Siemens and is supported by the Chinese companies Huawei and Lenovo. China is developing 4G mobile technology.

China's government pursues an aggressive development path to become a high technology leader but its approach emphasizes Chinese technologies, and the companies that develop them, as the core of any future standards. China's approach is the result of long-term planning, policy implementation and funding. In other words, government direction—supported by policy, politics, and generous subsidies—is driving China's tech development.

We should not assume that China will adopt "Western ideals" or business practices and take China's government at their word when they promise "reform" or a version of that. We need to determine what our interests are and assess them against what China has actually done over the years and what it ***says*** it wants to do.

I will leave it to my industry colleagues to discuss the technical issues relating to 5G and some of the implications. But, China has a well-defined and advanced approach to becoming a world-class player in this technology. China is poised to have a significant share of the global market in this and many other technologies.

China is now a leading technology power. In 2017, the U.S. ran a trade deficit in Advanced Technology Products (ATP) of $135.4 billion,[1] and our deficit for 2018 is expected to beat that when the full year trade statistics are released. For the narrower category of information and communications products, for October 2018 year-to-date figures (the latest available), the U.S. exported $3.365 billion and imported $130.303 billion. China has produced the faster supercomputer on earth. It is advancing quantum computing with rapid gains in cryptography and communications. It is excelling in artificial intelligence (AI) and a variety of other sectors.

Our failure to sell more in China is a direct result of their protectionist and predatory practices, including a goal, as identified in numerous policy documents, to develop indigenous capabilities to the exclusion of foreign players. As the Commission's 2018 Report indicated (summarized):

- Chinese IP requirements: Since 2007, China's Multi-Level Protection Scheme, which covers around 140,000 information systems,[2] requires Chinese IP in core IT technology and components and annual testing, certification, and authentication for the top three of the five tiers of IT users,[3] effectively excluding foreign competitors unless there is no domestic equivalent.[4] Article 34 of the draft guidelines would expand this scheme to

[1] Robert Scott and Zane Mokhiber, *The China Toll Deepens*, Economic Policy Institute, October 23, 2018, p. 31.
[2] The ranking is based on technology innovation, brand influence, ecosystem openness, and input from industry experts and end users. IoT One, "2018 Top 500 Industrial IoT Companies." https://www.iotone.com/iotone500. For more information on China's efforts to develop its semiconductor industry, see U.S.-China Economic and Security Review Commission, Chapter 1, Section 3, "China's 13th Five-Year Plan," in *2016 Annual Report to Congress*, November 2016, 155–161.
[3] The Multi-Level Protection Scheme separates information systems into five levels based on impact. Damage to a Level 1 (the lowest) information system could result in harm to legal rights of citizens, legal persons, or other organizations without harming national security, social order, or public interest. Damage to a Level 5 (the highest) information system results in very serious harm to national security. Level 3 and above encompasses finance, banking, tax, customs, commerce, communications, health, education, and social services. Nick Marro, "The 5 Levels of Information Security in China," China Business Review, December 6, 2016; Adam Segal, "China, Encryption Policy, and International Influence," Hoover Institution, No. 1610, November 28, 2016.
[4] China's Ministry of Public Security, Ministry of Public Security Draft for Comment for Multi-Level Protection Scheme on Internet Security, June 27, 2018. Translation.
http://www.mps.gov.cn/n2254536/n4904355/c6159136/content.html; Lance Noble, "Marshalls over Markets: China Tightens Cybersecurity," Gavekal Dragonomics, June 4, 2018, 9–10.

cloud computing platforms, big data systems, industrial control systems and mobile networks, AI, and IoT devices.[5]

- High restrictions on foreign ownership and investment: Under China's 2016 Telecommunications Regulations, foreign firms can own up to 50 percent of Chinese telecommunications and cloud computing providers.[6] China's 2016 Telecom Services Catalogue requires foreign telecommunications and cloud computing firms wishing to sell in the Chinese market to form joint ventures with Chinese firms.[7]
- China-specific technical standards: The Mercator Institute for China Studies (MERICS) found "China sometimes formulates national standards in strategic industries that deliberately differ from international standards in order to impede market access for foreign technology and to favor Chinese technology on the domestic market."[8]
- Restrictions on data storage and transfer: Under China's Cybersecurity Law, U.S. firms face significant restrictions on data storage and cross-border transfers—essential services for IoT devices. U.S. firms such as IBM, Apple, and Microsoft are required to form joint ventures with Chinese partners in order to operate.[9] In addition, foreign firms must rely on domestic partners and government-approved encryption technology, potentially placing foreign IP and data at risk.[10]

Huawei and ZTE, deemed "national champions" by the Chinese government, are global players in the communications field—from handsets to routers to switching to full network deployment and operations. And, as is well known, much of the production of telecom and IT products for leading firms is produced in China, or has components produced there.

Of course, not everything is a zero-sum game. Should we be concerned about where the products and services supporting and utilized in our 5G networks are produced and which

[5] China's Ministry of Public Security, "Ministry of Public Security Draft for Comment for Multi-Level Protection Scheme on Internet Security, June 27, 2018. Translation. http://www.mps.gov.cn/n2254536/n4904355/c6159136/contnt.html; Lance Noble, "Marshalls over Markets: China Tightens Cybersecurity," Gavekal Dragonomics, June 4, 2018, 11.

[6] BSA, "RE: China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation (Docket No. USTR–2017–0016)," September 28, 2017; Scott Thiel, "Telecommunications Laws of the World: China," DLA Piper, May 25, 2017.

[7] BSA, "Special 301 Submission," February 8, 2018; Gidon Gautel, "Establishing a Data Center in China," China Briefing, July 26, 2017; Norton Rose Fulbright, "China's New Telecom Catalogue Comes into Force on March 1, 2016," February 2016; Renee Barry and Matthew Reisman, "Policy Challenges of Cross-Border Cloud Computing (May 2012)," Journal of International Commerce and Economics 4:2 (November 2012).

[8] Jost Wübbeke et al., "Made in China 2025: The Making of a High-Tech Superpower and Consequences for Industrial Countries," Mercator Institute for China Studies, December 2016, 56.

[9] Samm Sacks and Manyi Kathy Li, "How Chinese Cybersecurity Standards Impact Doing Business in China," Center for Strategic and International Studies, August 2018; Lance Noble, "Marshalls over Markets: China Tightens Cybersecurity," Gavekal Dragonomics, June 4, 2018; Nick Marro, "Decoding China's Approach to Data Security," Diplomat, December 10, 2016; Daniel Castro and Alan McQuinn, "Cross-Border Data Flows Enable Growth in All Industries," Information Technology and Innovation Foundation, February 2015.

[10] Samm Sacks and Manyi Kathy Li, "How Chinese Cybersecurity Standards Impact Doing Business in China," Center for Strategic and International Studies, August 2018; Lance Noble, "Marshalls over Markets: China Tightens Cybersecurity," Gavekal Dragonomics, June 4, 2018, 9.

companies produce them? Should we have similar concerns about what other countries around the globe do in this regard?

Does that matter to us? I believe it does, in many ways.

The lead front-page article in the New York Times Sunday edition two weeks ago was entitled "*U.S. Scrambles to Outrun China in New Arms Race: Seeking to Restrict Beijing's Control Over 'Central Nervous System for Internet'*".[11] The stakes are, indeed, enormous.

5G will be the backbone of tomorrow's economy and infrastructure, including critical infrastructure; our telecommunications, e-commerce, and manufacturing sectors, along with many military and intelligence assets, will all depend on it. Technologies as diverse as the IoT, autonomous vehicles, cellular communications, and battlefield communications, will be built on 5G foundations.

The National Intelligence Council (NIC) released a report on the expected impact of 5G, finding it "will change the technological, social, and economic processes for a wide variety of industries by 2020."[12] By 2035, the NIC report predicted, $12.3 trillion in global economic output will be enabled by 5G tech, and its value chain will create $3.5 trillion in output and support 22 million jobs by 2035.

China's government clearly sees the future economic and security potential of 5G and is poised to invest at least $400 billion into its development. But that's only the tip of the iceberg. The communications and IT sectors are identified for preference and promotion as part of the Made in China 2025 industrial policy program, which means every province, local, and municipal government is marshalling its resources in response to the central government's directives.

China is also actively promoting its technological interests through its involvement in international standards-setting organizations, which will write the rules for interoperability and operations. It's part of their official government and Chinese Communist Party plans. China's government has already announced that its principal domestic suppliers—Huawei and ZTE—with each being allocated one-third of the market, leaving foreign competitors to scramble for the remaining third.[13]

China has aggressively participated in standards-setting bodies such as the International Telecommunications Union (ITU) where they play a significant role, as well as chair several

[11] The New York Times, *U.S. Scrambles to Outrun China in New Arms Race: Seeking to Restrict Beijing's Control Over 'Central Nervous System for Internet'*, January 27, 2019, p. 1.
[12] Next Generation Wireless Technologies to Change Industries, National Intelligence Council Report, September 12, 2017. NICR 2017-55.
[13] Eric Auchard and Sijia Jiang, *China's Huawei Set to Lead Global Charge to 5G Networks*, Reuters, February 23, 2018.

committees.[14] For several years, they have sent large delegations to these meetings hoping to drive standards that will advantage their own indigenous firms. This is contrary to the approach taken by many countries and industry delegations at the ITU and other international standard bodies who are seeking, first, to develop the standard that will create the most robust technologies and then seek to identify the best suppliers to meet those standards.

China is integrating its 5G plans with its Belt and Road Initiative (BRI) strategy. The 2015 Belt and Road Initiative White Paper,[15] which was jointly issued by China's National Development and Reform Commission, Ministry of Foreign Affairs, and Ministry of Commerce, calls for cross-border optical cables and communications trunk line networks, planning transcontinental submarine optical cable projects, and improving spatial and satellite information passageways to expand information exchanges and cooperation. The Chinese government is also actively seeking to loop its BRI partners into its "super-fast broadband network infrastructure" built in line with the Internet Plus plan.[16]

There is no comparable approach from our federal government. While a document leaked from the National Security Council identified the idea for the development and deployment of a federal 5G Internet, that approach appears to have been quickly abandoned based on industry opposition. Our country's current approach is market-led and market driven.

The Administration and Congress have adopted a number of security-related limitations to advance our interests. Just this past summer, Congress, as part of the National Defense Authorization Act for Fiscal Year 2019 adopted strict limitations on the procurement or renewal of contracts that include Huawei and ZTE equipment in government networks.[17] In the past, a variety of other measures have been put in place to limit the exposure of critical information and networks to Chinese cyberespionage. For example, the FY 2013 Appropriations bill prohibited Commerce, Justice, NASA and the National Science Foundation from acquiring information technology systems that were produced, manufactured or assembled by entities owned, directed or subsidized by the Chinese government.[18]

Huawei, as one of China's leading firms in this area, has received substantial attention. Today's hearing, of course, is about 5G, but it would be impossible to discuss that technology, and concerns vis-à-vis China, without commenting on Huawei. But Huawei must not be the only focus of the discussion of China's impact on 5G here in the U.S. and around the globe as there

[14] U.S.-China Economic and Security Review Commission, *2018 Report to Congress*, 115th Congress, Second Session, November 2018, p. 454.
[15] Vision and Actions on Jointly Building Silk Road Economic Belt and 21st-Century Maritime, Silk Road, March, 28, 2015, http://en.ndrc.gov.cn/newsrelease/201503/t20150330_669367.html.
[16] China needs to develop e-commerce, industrial networks, Internet banking: Ren, July 27, 2015, China Daily, http://english.gov.cn/news/top_news/2015/07/17/content_281475148857772.htm.
[17] Public Law 115-232, Sec. 889 – Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment.
[18] 2013 Consolidated and Further Appropriations Act (P.L. 113-6) (Sec. 516).

are many other vulnerabilities that must be addressed. Documented problems, such as China Telecom's redirection of Internet traffic through China, have been identified.[19]

Huawei Technologies is the most well-known Chinese telecommunications equipment company with operations and activities in the U.S. and has been cited as an advanced persistent threat to U.S. interests. In 2012, the House Permanent Select Committee on Intelligence identified strong concerns about Huawei and ZTE. The report concluded that "the risks associated with Huawei and ZTE's provision of equipment to U.S. critical infrastructure could undermine core US national-security interests."[20]

In early 2015, the FBI circulated a Counterintelligence Strategic Partnership Intelligence Note focused on national security risks associated with Huawei. That memo has been made public and included the following risk overview:

> *With the expanded use of Huawei Technologies Inc. equipment and services in U.S. telecommunications service provider networks, the Chinese Government's potential access to U.S. business communications is dramatically increasing. Chinese Government-supported telecommunications equipment on U.S. networks may be exploited through Chinese cyber activity, with China's intelligence services operating as an advanced persistent threat to U.S. networks. Huawei has been identified publicly for selling or attempting to sell U.S. intellectual property to export restricted countries (Iran/Cuba), making it a clear threat through its targeting of U.S. economic and proprietary information. China makes no secret that its cyber warfare strategy is predicated on controlling global communications network infrastructure.*[21]

According to press accounts U.S. Tier 1 telecom providers were counseled by officials of the U.S. government that utilization of Huawei equipment could create significant cybersecurity concerns and might jeopardize contracts with the U.S. government. Subsequently, each company reportedly decided not to procure equipment from the company for utilization on their networks.[22]

In 2018, the heads of the CIA, FBI, NSA, DIA, NGA and the Director of National Intelligence publicly testified as to their concerns about utilizing products or services from Huawei. FBI Director Wray stated,

> *We're deeply concerned about the risks of allowing any company or entity that is beholden to foreign governments that don't share our values to gain positions of power inside our telecommunications networks….it provides the capacity to exert pressure or*

[19] China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking, by Chris Demchak and Yval Shavitt, Military Cyber Affairs, 2018.
[20] Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE, HPSCI, October 8, 2012.
[21] Counterintelligence Strategic Partnership Intelligence Note (SPIN), Huawei, Federal Bureau of Investigation, February, 2015. (SPIN - 15-002)
[22] Lublin, Joann and Raice, Shayndi, Security Fears Kill Chinese Bid in U.S., The Wall Street Journal, November 2010.

> *control over our telecommunications infrastructure. It provides the capacity to maliciously modify or steal information. And it provides the capacity to conduct undetected espionage.*[23]

China's Huawei has been aggressive in trying to counter claims that it is a security risk. It claims that it is a private, employee-owned company and that we shouldn't worry. But, in recent months, a number of other countries—those who are part of the Five-Eyes relationship and others—have joined in questioning the security of Chinese-company produced equipment and whether it should be utilized in existing or future networks.

As William R. Evanina, the director of the National Counterintelligence and Security Center was quoted in the *New York Times*,

> *It's important to remember that Chinese company relationships with the Chinese government aren't like private sector company relationships with governments in the West…China's 2018 National Intelligence Law requires Chinese companies to support, provide assistance and cooperate in China's national intelligence work, wherever they operate.*[24]

No Chinese commercial entity can refuse to cooperate with China's security services. In 2017, China's government implemented a draconian Cybersecurity Law—despite the outcry from foreign governments and industry that it would raise serious concerns about the impact on the business activities of Chinese companies. The accompanying set of laws—National Intelligence Law of 2017, Counter-Terrorism Law of 2016, National Security Law of 2015 all raise concerns about Chinese entities freedom to act without government interference, coercion and direction.

Other countries have come to similar conclusions, based on their own assessments. For example, last July the United Kingdom's Huawei Oversight Board raised its concerns in a report to that country's national security advisor—despite 4 years of work with Huawei:

> "Due to areas of concern exposed through the proper functioning of the mitigation strategy and associated oversight mechanisms, the Oversight Board can provide only limited assurance that all risks to UK national security from Huawei's involvement in the UK's critical networks have been sufficiently mitigated. We are advising the National Security Adviser on this basis."[25]

I worry about China's approach, and its implications for us, for several reasons.

First, I approach this as someone who has always taken pride in America's technological leadership and do not want to cede it to any other country, especially when that leadership results from state-directed policies and support.

---

[23] Testimony before the Senate Select Committee on Intelligence, February 13, 2018.
[24] The New York Times, U.S. Scrambles to Outrun China in a New Arms Race, Sunday, January 27, 2019.
[25] Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report 2018, A report o the National Security Advisor of the United Kingdom, July 2018.

Second, I care about the production and jobs that will be created during the development, deployment and servicing of 5G networks. As the National Intelligence Council report indicated, $12.3 trillion in economic value will be created along with 22 million jobs. I want the bulk of that value and the jobs to advantage our economy and our people or at least know that the competition is being waged on a level-playing field.

Third, and most fundamental, I worry about our nation's security—economic, critical infrastructure and "traditional" security interests. On the economic side, we have read too many stories about Chinese cyberespionage, some facilitated and allegedly directed by the state, to steal our intellectual property. The fruits of that cyberespionage is estimated to have cost us hundreds of billions of dollars while advancing China's economic development and strength.

Financial networks, smart cities, power plants, dams, chemical production facilities, air traffic and so many other sectors are supported by the Internet and will be increasingly dependent on 5G with the dispersion of IoT devices. If Chinese companies provide the equipment, with control over the source code, the updates, and servicing, it creates extreme vulnerabilities.

Equally important, our warfighters and our defense sector are increasingly dependent on the electronic spectrum for command and control, logistics and other needs. China's military doctrine relies on "asymmetric warfare" where they have identified the electronic and space domains as critical to their countering any U.S. capabilities in a potential conflict. Access to or control over significant parts of our telecommunications systems and the connectivity that will be an increasingly important component for our defense systems can create substantial and, potentially, unacceptable vulnerabilities.

In its 2018 Annual Report, the Commission identified the following key findings, regarding this critical area:

- The Chinese government has strengthened its strategic support for the IoT (physical devices embedded with sensors that can collect data and connect to each other and the broader internet) and fifth-generation wireless technology (5G) networks. The government has laid out comprehensive industrial plans to create globally competitive firms and reduce China's dependence on foreign technology through: significant state funding for domestic firms and 5G deployment, limited market access for foreign competitors, China-specific technical standards, increased participation in global standards bodies, localization targets, and alleged cyber espionage and intellectual property theft. This state-directed approach limits market opportunities for foreign firms in China and raises concerns about the ability of U.S. and other foreign firms to compete fairly both in China's domestic market and abroad.

- 5G networks are expected to quicken data speeds by 100 times, support up to 100 times more IoT devices, and provide near-instant universal coverage and availability. U.S. and Chinese companies are engaged in a fierce competition to secure first mover advantage

and benefit from the trillions in economic benefits 5G and subsequent technologies are expected to create.

- IoT devices collect enormous amounts of user information; when aggregated and combined with greater computing power and massive amounts of publicly available information, these data can reveal information the user did not intend to share. U.S. data could be exposed through unsecure IoT devices, or when Chinese IoT products and services transfer U.S. customer data back to China, where the government retains expansive powers to access personal and corporate data.

- The Chinese government is leveraging its comparative advantage in manufacturing and state-led industrial policies to secure an edge in the IoT's wide-ranging commercial and military applications. U.S. firms and the U.S. government rely on global supply chains that in many cases are dominated by China. While not all products designed, manufactured, or assembled in China are inherently risky, the U.S. government lacks essential tools to conduct rigorous supply chain risk assessments. Federal procurement laws and regulations are often contradictory and are inconsistently applied.

- International 5G standards will be set by 2019, facilitating large-scale commercial deployment expected by 2020. The Chinese government is encouraging its companies to play a greater role in international 5G standards organizations to ensure they set global standards; such leadership may result in higher revenues and exports from internationally accepted intellectual property and technology and more global influence over future wireless technology and standards development.

- China's central role in manufacturing global information technology, IoT devices, and network equipment may allow the Chinese government—which exerts strong influence over its firms—opportunities to force Chinese suppliers or manufacturers to modify products to perform below expectations or fail, facilitate state or corporate espionage, or otherwise compromise the confidentiality, integrity, or availability of IoT devices or 5G network equipment. • The lax security protections and universal connectivity of IoT devices create numerous points of vulnerability that hackers or malicious state actors can exploit to hold U.S. critical infrastructure, businesses, and individuals at risk. These types of risks will grow as IoT devices become more complex, more numerous, and embedded within existing physical structures. The size, speed, and impact of malicious cyber attacks against and using IoT devices will intensify with the deployment of 5G.

The Commission made two recommendations for Congress to consider:

- Congress require the Office of Management and Budget's Federal Chief Information Security Officer Council to prepare an annual report to Congress to ensure supply chain

vulnerabilities from China are adequately addressed. This report should collect and assess:

  - Each agency's plans for supply chain risk management and assessments;
  - Existing departmental procurement and security policies and guidance on cybersecurity, operations security, physical security, information security, and data security that may affect information and communications technology, 5G networks, and IoT devices; and
  - Areas where new policies and guidance may be needed—including for specific information and communications technology, 5G networks, and IoT devices, applications, or procedures—and where existing security policies and guidance can be updated to address supply chain, cyber, operations, physical, information, and data security vulnerabilities.

- Congress direct the National Telecommunications and Information Administration and Federal Communications Commission to identify (1) steps to ensure the rapid and secure deployment of a 5G network, with a particular focus on the threat posed by equipment and services designed or manufactured in China; and (2) whether any new statutory authorities are required to ensure the security of domestic 5G networks.

The impending rollout of 5G here in the U.S. and across the globe requires that we address these vulnerabilities quickly and aggressively. In my view it is better to err on the side of safety, as 5G will be the backbone of communications in the future. We cannot afford to ignore the actions and activities that China has engaged in with regard to predatory and protectionist policies, what their public pronouncements have identified are their plans and what actions they have engaged in in the cyber realm.

We also have to be realistic about the global nature of production and what the limits are on our policies and actions. But, the price of inaction is unacceptable. We must protect our interests where we can and manage and mitigate the risks where we must.

###