Questions for the Record Submitted to
Deputy Assistant Secretary Robert Strayer by
Chairman Lindsey Graham (No. 1 to No. 2)
U.S. Senate Committee on the Judiciary
May 14, 2019

Question 1:

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

Answer 1:

The Department has several concerns with the pricing and financing of Huawei products, which are supported by the Chinese government, including with low or no interest loans from state-owned banks. Chinese state support on non-commercial terms indicates that Beijing has strategic interests at play. We know that the success of Chinese 5G vendors is a goal of Xi Jinping's signature policy initiatives like the Digital Silk Road. The Digital Silk Road is part of both the One Belt, One Road strategy to expand China's state-centric model of internet governance and the "Made in China 2025" industrial plan for achieving Chinese global dominance of high-tech sectors, including 5G. This support distorts market dynamics and puts undue pressure on qualified vendors who are competing fairly. We worry that this predatory behavior could result in market exits for companies that cannot sustain non-commercial pricing structures, leaving state-supported Chinese vendors dominant in a sector of critical importance to our national security, economic competitiveness, and core values.

Questions for the Record Submitted to
Deputy Assistant Secretary Robert Strayer by
Chairman Lindsey Graham (No. 1 to No. 2)
U.S. Senate Committee on the Judiciary
May 14, 2019

Approved:	EB/FO: Peter Haas	(ok)
Drafted:	EB/CIP/TS – Doug May, ext. 7-5835 and cell: 202-341-0941	
Cleared:	EB/FO: Rebekah Huskamp	(ok)
	EB/CIP: Jonathan Fritz	(OK)
	D: Elizabeth Hattingh	(OK)
	E: Leila Elmergawi	(OK)
	H: Daniel McCartney	(OK)
	P: Jason Hwang	(OK)
	R: Nancy Talbot	(OK)
	S/P: Evan Ellis	(OK)
	T: Joanna LaHaie	(OK)
	EAP/CM: Bon Fleming	(OK)
	EAP/P: Connie Chung	(OK)
	GPA: Beth Robbins	(OK)
	ISN/CATR: David Aron	(OK)
	L/EB: Benjamin Levin	(OK)
	SCCI: Sheila Flynn	(OK)

Questions for the Record Submitted to
Deputy Assistant Secretary Robert Strayer by
Chairman Lindsey Graham (No. 1 to No. 2)
U.S. Senate Committee on the Judiciary
May 14, 2019

Question 2:

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?

Answer 2:

The Department of Commerce action to place Huawei on the Entity List is a separate and distinct action from the Executive Order on "Securing the Information and Communications Technology and Services Supply Chain."

Effective May 16, 2019, the Commerce Department placed Huawei and 68 non-U.S. affiliates of Huawei on the Entity List. This regulatory action is based on reasonable cause to believe Huawei has been involved in activities contrary to the national security or foreign policy interests of the United States, such as its alleged transfers of technology to Iran in violation of U.S. sanctions restrictions.

On May 15, the President signed the Executive Order on "Securing the Information and Communications Technology and Services Supply Chain" to protect the security, integrity, and reliability of information and communications technology and services provided and used in the United States. The Executive Order is directed at transactions involving any information and communications technology or service that is designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary and that meet additional enumerated criteria. The Executive Order directs the Secretary of Commerce to issue implementing rules or regulations within 150 days of the date of the Executive Order.

Questions for the Record Submitted to
Deputy Assistant Secretary Robert Strayer by
Chairman Lindsey Graham (No. 1 to No. 2)
U.S. Senate Committee on the Judiciary
May 14, 2019

With regard to export control laws and patents, exports and re-exports of technology in the form of a patent application may require an application with the U.S. Patent and Trademark Office or may otherwise be required to comply with the U.S. export control law.

Questions for the Record Submitted to
Deputy Assistant Secretary Robert Strayer by
Chairman Lindsey Graham (No. 1 to No. 2)
U.S. Senate Committee on the Judiciary
May 14, 2019

Approved:	EB/FO: Peter Haas	(ok)
Drafted:	EB/CIP/TS – Doug May, ext. 7-5835 and cell: 202-341-0941	
Cleared:	EB/FO: Rebekah Huskamp	(ok)
	EB/CIP: Jonathan Fritz	(OK)
	D: Elizabeth Hattingh	(OK)
	E: Leila Elmergawi	(OK)
	H: Daniel McCartney	(OK)
	P: Jason Hwang	(OK)
	R: Nancy Talbot	(OK)
	S/P: Evan Ellis	(OK)
	T: Joanna LaHaie	(OK)
	EAP/CM: Bon Fleming	(OK)
	EAP/P: Connie Chung	(OK)
	GPA: Beth Robbins	(OK)
	ISN/CATR: David Aron	(OK)
	L/EB: Benjamin Levin	(OK)
	SCCI: Sheila Flynn	(OK)

Questions for the Record Submitted to
Deputy Assistant Secretary, Rob Strayer by
Senator Chuck Grassley (No. 1 to No.3),
U.S. Senate Committee on the Judiciary
May 14, 2018

Question 1:

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?

Answer 1:

The U.S. Department of State (DOS) defers to the U.S. Department of Homeland Security (DHS) on this matter.

Question 2:

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?

Answer 2:

DOS defer to DHS on this matter.

Question 3:

The Administration signed an executive order on May 15, the day after the Judiciary Committee held this 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):"

a. Does the State Department support this Executive Order?

b. Will the State Department 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?

c. How does this Executive Order impact our foreign allies?

Answer:

3a) Let me assure you that the Department of State fully supports this Executive Order (EO) as a vital mechanism to help ensure the continued security, prosperity, and technological leadership of the Unites States.

3b) The Department is a full interagency partner in the NSC-led coordination process to implement this EO. We are proud to be part of a committed team of U.S. government stakeholders advising in the drafting of the related rules, as well as processes to evaluate and address supply chain risks and threats.

3c) Many of our foreign allies and partners are seeing a link between potential risks to their national economies and threats from any compromise of their communications supply chains, which they are now considering how best to secure. As our allies and partners consider their next steps, we are engaging them on our own approach as laid out in Executive Order while sharing appropriate supporting information and intelligence, in close coordination with our U.S. interagency colleagues.

Approved: EB/FO – Acting A/S Peter Haas PDH

Drafted: EB/CIP/TS – Joe Burton ext. 7-5231 and cell: 410-804-6199

Cleared:

EB/CIP: Robert Strayer	(ok)
EB/CIP/BA: Jonathan Fritz	(ok)
EB/CIP/TS: Jabin Vahora	(ok)
EB/OIA: Patrick Chow, Ben Ford	(ok)
EB/IPE Tarek Fahmy.	(ok)
EB/TPN/BTA: Archana Poddar	(ok)
EB/EPPD: Anna Balogh, Ace Gazis	(ok)
L/EB: Michael Aktipis	(ok)
D: Elizabeth Hattingh	(ok)
P: Jason Hwang	(ok)
S/P: Duncan Walker	(ok)
E: Leila Elmergawi	(ok)
H: Daniel McCartney	(ok)
R: Emily Armitage	(ok)
GPA/PL/PE: Jennifer Schaming	(ok)
GPA/FO Elizabeth Robbins	(ok)
EAP/CM: Bon Fleming	(ok)
INR: Jason Weinberg	(ok)

Questions for the Record Submitted to
Deputy Assistant Secretary Rob Strayer by
Senator John Cornyn (No. 1 to No. 5)
U.S. Senate Committee on the Judiciary
May 14, 2019

Question 1:

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?

Answer 1:

Innovation and market discipline make U.S. firms world leaders in many parts of the 5G ecosystem, from semiconductors and smartphones to routers and servers, and we expect they will be competitive in developing and deploying other emerging technologies such as AI and IOT. Our companies continue to be market leaders throughout the ICT ecosystem and this shows the strength of the U.S. market-based approach. At the same time, the USG is taking action to address the unfair Chinese trade practices.

Question 2:

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

Answer 2:

DOS defers to DHS on this matter.

Question 3:

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?

Answer 3:

Yes. The pilot program applies to certain investments by foreign persons in U.S. businesses that are involved with one or more critical technologies related to 27 enumerated sensitive industry sectors. Each of the industry sectors you mentioned are included.

Question 4:

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?

Answer 4:

I believe the security of information and communications technology (ICT) networks and services is a critical element of national security. ICT plays a crucial role in the safety, security, and prosperity of all nations and is thus an attractive target for foreign adversaries and malicious cyber actors. Executive Order 13873 entitled "Securing the Information and Communications Technology and Services Supply Chain" underscores how seriously the Administration takes its commitment to secure the ICT supply chain from efforts by foreign adversaries to create and exploit vulnerabilities. Protecting sensitive technology and intellectual property is a global challenge most likely to be realized through robust investment review mechanisms, such as CFIUS in the United States, multilateral export control regimes, and enhanced information sharing and collaboration among like-minded nations.

Question 5:

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?

Answer 5:

DOS defers to DHS on this matter

Questions for the Record Submitted to
Deputy Assistant Secretary Robert Strayer by
Senator Ben Sasse (No. 1 to no. 6)
U.S. Senate Committee on the Judiciary
May 14, 2019

Question 1:

Can you clarify the relationship between Huawei, ZTE, and Chinese tech companies and the Chinese Communist Party? How do the interests of one serve the other?

Answer 1:

China is a one party state with no formal checks or balances on its ability to compel citizens or companies to cooperate with its security and intelligence agencies. This is codified in Chinese legislation such as the National Security Law, the National Intelligence Law, the Counter-Terrorism Law, and the Cybersecurity Law. These make clear that if a Chinese company, regardless of whether it is state-owned or private, is directed to collaborate, it has no choice but to do so, and to keep such collaboration secret.

Question 2:

What are the implications for the United States and the global economy if China is able to win the race to 5G dominance?

Answer 2:

China seeks to establish itself as a cyber power and has been rapidly developing a legal framework to enhance its control over data, networks, and information in cyberspace. China's increasing willingness to use all the tools at its disposal poses a significant risk to global communications networks. Allowing telecommunications companies subject to Chinese jurisdiction to dominate international telecommunications networks (including infrastructure such as telephone lines, fiber optic cables, cellular networks, communication satellites, and data centers) would give them greater access to global data and the ability to exploit that access to the detriment of U.S. national security interests. Specifically, such access could be used to skim data and steal intellectual property, as well as to disrupt or turn off global communications networks.

Question 3:

Can you speak a bit more about how our allies and partners in Europe and Asia are thinking about the security implications surrounding 5G? How much do they share our concerns? Why do some of our traditional partners seem to be more accommodating to Huawei technology than we are?

Answer 3:

We have been working with our allies and partners to raise awareness the national security risks associated with using untrusted vendors in 5G networks. Countries around the world are acknowledging that supply chain security is critical to the overall security and reliability of their

future 5G networks. All countries, including our allies and partners, can and should make their own sovereign decisions with a full understanding of the risks and vulnerabilities involved.

Question 4:

How critical is it for our security that our allies have the same view of next generation of technology with a Chinese origin? What are the risks to the United States if they do not share the same view?

Answer 4:

The security of our communications networks is vital not only to U.S. national security, but to the security of our allies and partners. The United States government has been raising awareness among our allies and partners of the national security risks posed by untrusted telecoms equipment vendors like Huawei and ZTE that are subject to unchecked powers of compulsion by an authoritarian government.

Question 5:

What is it going to take for us to have a unified view across our alliances, particularly the NATO alliance?

Answer 5:

The Administration is engaging intensively with international partners, including NATO Allies, on the importance of safeguarding our 5G networks. We stress that the security of our Allies' telecoms networks has a direct bearing on our mutual national security. The presence of untrusted vendors in any of our next-generation wireless networks could impact our ability to share sensitive information and mobilization requirements. Allies have begun to consult on how NATO might approach its future engagement with and related to China. The United States strongly supports NATO doing more to counter potential Chinese threats. The United States also welcomes NATO-EU cooperation on the vulnerabilities posed by the use of Chinese equipment in telecommunications/5G networks. We see this as an area where NATO-EU cooperation would be beneficial given the complex and overlapping concerns between the military and civilian realm, and the overarching security implications for both organizations and for all NATO and EU members.

Question 6:

What is Putin’s view of 5G? How is he working to shape this tech race we are currently engaged in with the China?

Answer 6:

Questions for the Record Submitted to
Deputy Assistant Secretary Robert Strayer by
Senator Ben Sasse (No. 1 to no. 6)
U.S. Senate Committee on the Judiciary
May 14, 2019

In his annual address to the Federal Assembly in February 2019, President Putin identified 5G implementation as a priority for Russia. On June 6, at the Saint Petersburg International Economic Forum, Russia's flagship economic event, Russia's MTS and China's Huawei signed an agreement to build a 5G network in Russia. I am committed to safeguarding our 5G network, and will continue to monitor Russia and China's cooperation in this sphere, and assess how it affects U.S. network security.

Questions for the Record Submitted to
Deputy Assistant Secretary Robert Strayer by
Senator Thom Tillis (No. 1 and No.2)
U.S. Senate Committee on the Judiciary
May 14, 2019

Question 1:

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?

Answer 1:

Standards developed through open, transparent, and consensus-based processes ensure that national security, economic competitiveness, and technological innovation related considerations are appropriately considered and taken into account. Congress can ensure continued U.S. leadership in 5G standards development and protect U.S. national security in this area by: (1) Incentivizing participation by U.S. stakeholders, particularly early and mid-career technical experts who will be the future contributors and leaders, and (2) commit strong support for U.S.-led research and development that will serve as the foundation of future contributions by U.S. stakeholders as to 5G technology-related standards development.

Question 2:

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?

Answer 2:

Standards developed by Standards Development Organizations (SDOs) reflect the interests of the participating members. The ultimate adoption of these voluntary standards is also connected to the market-relevance, timeliness, and technical rigor of the development process. Ensuring that SDOs stay open and transparent to all interested stakeholders and continue to develop standards in consensus-based processes provides predictability to participants. Committed and consistent participation by experts – from both private sector and the government – ensures that technologies being considered for standards development are fit-for-purpose.

Questions for the Record Submitted to
Deputy Assistant Secretary Robert Strayer by
Senator Chris Coons (No. 1 to No. 3)
U.S. Senate Committee on the Judiciary
May 14, 2019

Question 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. 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?

Answer 1:

The President took a critical step to safeguard our national security by signing the Executive Order 13873 on "Securing the Information and Communications Technology and Services Supply Chain." At the same time, the Administration is acting to ensure that the United States remains a leader in wireless innovation by accelerating the development and deployment of 5G in the United States. A key part of this effort is the FCC's forward-looking, comprehensive strategy to Facilitate America's Superiority in 5G Technology (the 5G FAST Plan) by making more spectrum available to the market and cutting regulatory barriers. America is a global leader in 5G roll out, and U.S. firms are competitive in many parts of the 5G stack.

Question 2:

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?

Answer 2:

Standards developed through open, transparent, and consensus-based processes ensure that national security, economic competitiveness and technological innovation related considerations are all appropriately considered and taken into account. Congress can ensure continued U.S. leadership in 5G standards development and protect U.S. national security in this area by: (1) Incentivizing participation by U.S. stakeholders, particularly early and mid-career technical experts who will be the future contributors and leaders, and (2) commit strong support for U.S.-led research and development that will serve as the foundation of future contributions by U.S. stakeholders as to 5G technology-related standards development.

Questions for the Record Submitted to
Deputy Assistant Secretary Robert Strayer by
Senator Chris Coons (No. 1 to No. 3)
Senate Committee on the Judiciary
May 14, 2019

Question 3:

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?

Answer 3:

The United States can strengthen intellectual property protections and incentivize U.S. leadership in next-generation technologies by promoting policies that protect all types of intellectual property against misappropriation. By continuing to enforce patentability standards we ensure that U.S. innovators are able to protect their inventions with patents. U.S. innovators should also continue to feel confident that intellectual property enforcement procedures are available in the digital environment. As U.S. companies look internationally, the Administration will continue to advocate for high-standard intellectual property rights regimes and enforcement abroad.

Questions for the Record Submitted to
Deputy Assistant Secretary Robert Strayer by
Senator Cory Booker (No. 1 to No. 5)
U.S. Senate Committee on the Judiciary
May 14, 2019

Question 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?

Answer 1:

The State Department (DOS) defers to the Department of Homeland Security (DHS) on this matter.

Question 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.

Answer 2:

DOS defers to DHS on this matter.

Questions for the Record Submitted to
Deputy Assistant Secretary Robert Strayer by
Senator Cory Booker (No. 1 to No. 5)
U.S. Senate Committee on the Judiciary
May 14, 2019

Question 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:

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

b. 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?

c. 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?

Answer 3:

International standards play an important role in spurring innovation. The USG is paying close attention to China's role in international standards organizations. We want Chinese companies to participate in these industry-led international processes rather than creating their own standards unilaterally, which could lock U.S. companies out of the Chinese market. With regard to patents, the United States has earned a reputation for quality over quantity. We are confident that high-quality technology covered by high-quality patents will prevail in international standards bodies over low-quality technology covered by low-quality patents.

Question 4a

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?

Answer 4a:

DOS defers to DHS on this matter.

Question 4b:

b. 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?

Answer 4b:

Rather than relying on free markets, China uses market-distorting subsidies and other industrial policy tools in an effort to become self-reliant (and eventually dominant internationally) in high-tech sectors. The results have been mixed. The United States has placed Huawei and its subsidiaries on the Entity List because Huawei has engaged in activities contrary to U.S. national security and foreign policy interests, including violating U.S. export control laws. Additionally, Commerce has issued a temporary general license targeted to help innocent third parties utilizing Huawei equipment and services. We refer you to Commerce for more details.

Question 4c:

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

Answer 4c:

The United States does not seek a tech "Cold War." The United States is working vigorously to safeguard U.S. national security and ensure that U.S. intellectual property and technology are protected.

Questions for the Record Submitted to
Deputy Assistant Secretary Robert Strayer by
Senator Cory Booker (No. 1 to No. 5)
U.S. Senate Committee on the Judiciary
May 14, 2019

Question 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):

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

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

Answer 5:
DOS defers to DHS on this matter.