WRITTEN RESPONSES – QUESTIONS FOR THE RECORD

BRANDON J. PUGH, ESQ.
POLICY DIRECTOR & RESIDENT SENIOR FELLOW,
CYBERSECURITY & EMERGING THREATS
R STREET INSTITUTE

FOR THE

SUBCOMMITTEE ON INNOVATION, DATA, AND COMMERCE
COMMITTEE ON ENERGY AND COMMERCE
UNITED STATES HOUSE OF REPRESENTATIVES

HEARING ON

ECONOMIC DANGER ZONE: HOW AMERICA COMPETES TO WIN THE FUTURE VERSUS CHINA

FEBRUARY 1, 2023

Attachment 1—Additional Questions for the Record

The Honorable Larry Bucshon

1. *A July 2019 Inspector General's report found that the Department of Defense has purchased tens of millions of dollars of Commercial off the Shelf (COTS) technologies with known cybersecurity risks from IT firms in which the Chinese government has an ownership stake. What is the U.S. government doing to protect the U.S. military and other government departments and agencies against the risks associated with this behavior?*

   The 2019 Inspector General's report was alarming and highlighted what many suspected about Commercial off the Shelf (COTS) technologies, including that adversaries could exploit known cybersecurity vulnerabilities in COTS items purchased by the Department of Defense and other federal agencies. The 2023 National Cybersecurity Strategy notes that the federal government will continue to focus on software supply chain risk mitigation in federal civilian executive branch (FCEB) agencies and replace or update systems that are not defensible against sophisticated cyber threats. Executive Order 14028, "Improving the Nation's Cybersecurity," expressed similar themes.

   While COTS are not specifically named in either, I am hoping they are one aspect of the administration's implementation plan. Unfortunately, the issue is not isolated at the federal level because local and state entities often use these devices, including in K-12 schools.

2. *Although the State Department, Department of Defense, and several intelligence agencies have individually banned the purchase of computers and printers from companies in which the Chinese government has an ownership stake, these procurement guidelines are not standard across federal agencies. What steps is the Administration taking to close these widespread critical cybersecurity vulnerabilities?*

   A consistent approach is critical in addressing cybersecurity concerns that are present with both software and hardware made partially or fully by Chinese-backed or Chinese-owned companies. The 2023 National Cybersecurity Strategy furthers the call for technology modernization and eliminating legacy systems that are difficult to defend. I am hopeful that will entail removing concerning technology that already exists. Looking ahead, part of the strategy entails furthering EO 14028 to ensure "contract requirements for cybersecurity are strengthened and standardized across Federal agencies," along with enforcement when companies do not follow best practices. Specifics are not clear, but I am hopeful this will entail products with links to countries of concern like China.

3. *The computing division of the Chinese Academy of Sciences (CAS) was added to the U.S. government's Entity List in December 2022. Do you believe the U.S. government should continue to allow federal departments and agencies to purchase computers from other firms that CAS owns, or firms in which CAS has a significant ownership stake? Why or why not?*

   The Chinese Academy of Sciences Institute of Computing Technology was one of 36 entities added to the Entity List for "acting contrary to the national security or foreign policy interests of the United States." If an entity is on this list, we must be concerned and skeptical of other transactions by firms that are fully or partially owned by the entity so they cannot use a subsidiary as a workaround to exploit or create vulnerabilities. Availability, convenience and

cost are factors for purchasing these products, but those factors should not outweigh security risks. I recommend that the Department of Commerce conduct a review of all of these entities for potential additions to the Entity List.

The Honorable Neal Dunn

1. *A July 2019 Inspector General's report found that the Department of Defense continues to buy tens of millions of dollars in Commercial off the Shelf (COTS) technologies with known cybersecurity risks such as Lenovo computers, Lexmark printers, and GoPro cameras. What is the U.S. government doing to close loopholes that Lenovo and other IT firms in which the Chinese government has an ownership stake can exploit to sell its equipment to the U.S. military and other federal government departments and agencies?*

   The 2019 Inspector General's report was alarming and highlighted what many suspected about Commercial off the Shelf (COTS) technologies, including that adversaries could exploit known cybersecurity vulnerabilities in COTS items purchased by the Department of Defense and other federal agencies. The 2023 National Cybersecurity Strategy notes that the federal government will continue to focus on software supply chain risk mitigation in federal civilian executive branch (FCEB) agencies and replace or update systems that are not defensible against sophisticated cyber threats. Executive Order 14028, "Improving the Nation's Cybersecurity," expressed similar themes.

   While COTS are not specifically named in either, I am hoping they are one aspect of the administration's implementation plan. Unfortunately, the issue is not isolated at the federal level because local and state entities often use these devices, including in K-12 schools.

2. *Although the State Department, Department of Defense, and several intelligence agencies have banned the purchase of computers and printers from companies in which the Chinese government has an ownership stake, these procurement guidelines are not standard. What steps is the Administration taking to close these widespread critical cybersecurity vulnerabilities across the federal government?*

   A consistent approach is critical in addressing cybersecurity concerns that are present with both software and hardware made partially or fully by Chinese-backed or Chinese-owned companies. The 2023 National Cybersecurity Strategy furthers the call for technology modernization and eliminating legacy systems that are difficult to defend. I am hopeful that will entail removing concerning technology that already exists. Looking ahead, part of the strategy entails furthering EO 14028 to ensure "contract requirements for cybersecurity are strengthened and standardized across Federal agencies," along with enforcement when companies do not follow best practices. Specifics are not clear, but I am hopeful this will entail products with links to countries of concern like China.

3. *The computing division of the Chinese Academy of Sciences (CAS) was added to the U.S. government's Entity List in December 2022. Why does the U.S. government continue to allow federal departments and agencies to purchase computers from other firms that CAS owns? Why should a known security threat like Lenovo, in which CAS has a significant ownership stake that it tries to hide through subsidiary entities, be allowed to sell equipment to the U.S. federal government?*

The Chinese Academy of Sciences Institute of Computing Technology was one of 36 entities added to the Entity List for "acting contrary to the national security or foreign policy interests of the United States." If an entity is on this list, we must be concerned and skeptical of other transactions by firms that are fully or partially owned by the entity so they cannot use a subsidiary as a workaround to exploit or create vulnerabilities. Availability, convenience and cost are factors for purchasing these products, but those factors should not outweigh security risks. I recommend that the Department of Commerce conduct a review of all of these entities for potential additions to the Entity List.

4. *Which allies and partners should the US be working with to help diversify supply chains away from China?*

   Supply chain risks only continue to expand, especially considering we rely on countries like China for essential products and components. Bringing back more manufacturing to the United States is a key way to help mitigate cybersecurity risks, to make American companies more competitive and to reduce our reliance on countries of concerns. Relatedly, "friend-shoring" is a way to diversify and secure our nation's supply chain. This can empower countries that the United States has positive relations with, like our military allies, to produce products that we need without relying on concerning countries like China. This can also entail working with countries closer to the United States to help minimize supply chain risks like we have already done with Mexico.

The Honorable Greg Pence

I share your concerns of anti-competitive practices of the Chinese Communist Party and their efforts to undermine innovation here in the U.S. Rightfully so, companies across the world are re-thinking their partnerships with the CCP, who have spent decades cornering critical supply chains by stealing intellectual property and manipulating free markets.

As the U.S. continues re-building our domestic manufacturing base, foreign direct investment will be a critical tool to work alongside allied nations against the illegal subterfuge of China and bring good-paying jobs to communities in Indiana and across the country. Indiana is a national leader in attracting foreign direct investment from allied countries. Over 200,000 Hoosiers are employed by international companies, of which 56 percent are in the manufacturing sector. To continue fostering strong growth in these sectors, I introduced the Global Investment in American Jobs Act last Congress, which seeks to identify barriers to innovation and promote investment from our friends abroad to open new markets.

I am concerned, however, that China could be circumventing national security laws to gain footholds in domestic industries, particularly in next generation technologies. These efforts could threaten the security of our nation as well as the privacy of our citizens.

1. *In your view, how can foreign direct investment from allied nations be used as a tool to combat anti-competitive practices of the Chinese Communist Party?*

   Foreign direct investment (FDI) from allied nations can be helpful in combating anti-competitive practices of the Chinese Communist Party in two main ways. First, we see China being a large recipient of FDI and that strengthens China and its companies. It is important for the United States to foster an environment favorable for FDI to ensure we

outpace China on receiving FDI. Second, Chinese firms are eager to invest in the United States, which presents risks and strengthens a main rival. It is important to ensure our allies are empowered to push back against China.

2. *How can Congress secure the landscape of foreign direct investment from allied countries and prevent China from subverting national security laws to gain strongholds in domestic industries?*

   There are risks with FDI from firms that are directed, controlled or funded by select foreign governments like the Chinese Communist Party. FDI can be leveraged to make China stronger or even exploit security vulnerabilities. Congress should ensure a climate is created that fosters innovation from our allies, while ensuring that risky investments are properly vetted or avoided.

The Honorable Russ Fulcher

As a former Micron tech executive, I get the foreign subsidy challenge. I dealt with it against Japan in the 1980s, and others since. That is a part of dealing with various governments. What is different in this case is the level and systematic theft, and then subsidizing the technology from these ill-gotten gains.

As the Congressional Research Service (CRS) noted, China's strategy involves the "process of introducing, absorbing, and adapting" foreign technology and then "rebranding" that technology as its own.

The "One Belt, One Road" initiative is one way they do this. We know it includes requiring some industry sensitive information to be shared by the foreign company in a joint venture with a Chinese-backed company in China. But it also includes various types of collaboration centers, open technology grabs, and overseas academic and non-academic research centers.

1. *When it comes to basic research, what are things we can do to protect open source technology platforms, and are there areas in U.S. export control laws that need to be strengthened?*

   Open source software and related technologies offer benefits like fostering collaboration and access, but there can be cybersecurity risks. For example, a known vulnerability can be exploited to compromise data or an entire system, or software might be outdated. Also, we see Chinese developers contributing to open source projects. To combat this, it is important that entities are aware of known vulnerabilities, that United States' software manufacturers implement strong security and that we do not allow China to dominate open source efforts.

2. *When it comes to online research, I support the committee's efforts to move on legislation from the last Congress that would alert users who go to a website that is owned by the Chinese Communist Party. What next steps to secure online collaboration among researchers, or allow the U.S. to take actions against CCP-backed efforts to steal our IP? Emerging patent courts and laws in China?*

   Unfortunately, China's quest to steal United States' data is not new and it is an ongoing concern. This ranges from data on Americans to our intellectual property. Awareness of the threat is one key step. For example, a comprehensive data privacy and security law like the American Data Privacy and Protection Act (ADPPA) would alert individuals if their data is being transferred to select countries like China, which puts the individual on notice and allows them the option to proceed or not. Actions by law enforcement, federal agencies, and even the private sector must continue to help stop bad actors from stealing our data and property. This also entails making sure public and private sector entities are prepared and resourced, especially our smallest entities.

Much of the danger of using Chinese infrastructure and companies when research, development, and subsequent data from testing, comes from the potential for Chinese vendors to access information from the back end.

3. *Would there be benefits to creating a data reciprocity community, like a "Transparency Defensive Alliance" for corporate data sharing, for countries allied with western standards of corporate conduct and accountability and western values?*

   Creating a system or process for corporate data sharing could be a helpful tool for countries allied with western standards of corporate conduct, but there are many questions to answer first. A key threshold point is that there is always the risk for a bad actor to access and exploit data so this community would not be foolproof. This would require clarity on the type of data to be shared, security protections, how international laws would be implicated like those on data privacy, and access and monitoring rules, among other areas.

4. *Would it be beneficial to extend this sort of an agreement to encompass cloud storage and other services that may be shared with a host company or nation?*

   As the foundation and structure for a data reciprocity community are explored, I think encompassing cloud storage and other services that might be shared with a host country and/or nation is worth exploring.

Attachment 2—Member Requests for the Record

The Honorable Debbie Lesko

When a security camera that was made in China is connected to wireless internet in the United States, have there been instances where this information has been transmitted back to China?

There are many software and hardware products that pose risks like connected devices. For example, there are reports of baby cameras spying on children, electronic locks being remotely opened and robot vacuum cleaners recording people in the bathroom. Some manufacturers implement strong privacy and security measures, but that is not the case for all and many devices lack even basic security measures.

Even more troubling, there is a lack of clarity about what is and is not accessible in China. With so many Internet of Things (IoT) devices made fully or partially in China, it is possible for the data to be collected and harvested in China. We have seen cases where Chinese-made cameras with security vulnerabilities have permitted remote access and eavesdropping. Options to help address these concerns include acting on a comprehensive data privacy and security law, advancing an IoT label for consumers and furthering IoT security baselines.

The Honorable Kat Cammack

How can we protect our kids and data while simultaneously respecting free market economics?

Acting on a comprehensive data privacy and security law, like the American Data Privacy and Protection Act (ADPPA) from the last Congress, is the best way to protect our kids and data. While there are bills specifically aimed at protecting kids, a comprehensive approach would simultaneously protect kids and all Americans. Threats to our data continue to increase so it is critical that the threat be dealt with for all.

A comprehensive bill would also better assist companies of varying sizes so they would have one law to follow, rather than the growing patchwork of state laws that is becoming a compliance nightmare and resource drain. When legislation is contemplated, it should consider businesses of all sizes, include strong preemption language, and be based on achieving compliance rather than being enforcement-heavy.