House Energy & Commerce Subcommittee on Innovation, Data, and Commerce
Additional Questions Submitted for the Record
Samm Sacks

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?

Answer: My understanding is that there are range of mandated requirements for ICT products used by the U.S. government and military when it comes to supply chain security, but answering what the DOD is doing specifically on IT purchases of COTS is beyond my area of expertise and focus of my research. I also encourage the Administration to further examine and review areas of the supply chain that present vulnerabilities that may not be covered and merit additional scrutiny and restrictions.

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?

Answer: I do not know the answer to this question. Please see response above.

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?

Answer: The Chinese Academy of Science holds the status of a government Ministry in China. It is a powerful and influential research institute connected with senior government leadership and involved with directing science and technology policy. I am not familiar with the specific division or subsidiary firm that sells computers, but my understanding is that any firm listed on the U.S. government's Entity List has been identified for restrictions on sales or transfer of U.S. technology due to a preponderance of evidence that the entity has connections to actors in the government or military in China that pose U.S. national security risks. While the Entity List would not itself restrict purchasing technology from any identified firm, the fact that any firm is listed there reflects there are factors of concern related to U.S. national security that should be factored into any sensitive commercial or U.S. government procurement decisions.

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?

Answer: I do not know what specific steps the U.S. government is taking regarding purchases from Lenovo, Lexmark, and GoPro cameras. I have not researched these specific companies and their associated cybersecurity risks.

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 in the Administration taking to close these widespread critical cybersecurity vulnerabilities across the federal government?

Answer: The question of U.S. government procurement of computers and printers in relation to China is not something I have looked at in depth. I applaud the Administration for its recently released National Cybersecurity Strategy and its efforts to close critical cybersecurity vulnerabilities across several areas, including mandated cybersecurity requirements (beyond recommended standards), security by design, and examining loopholes and unaddressed vulnerabilities tied to market incentives.

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?

Answer: The Chinese Academy of Science holds the status of a government Ministry in China. It is a powerful and influential research institute connected with senior government leadership and involved with directing science and technology policy. I am not familiar with the specific division or subsidiary firm that sells computers, but my understanding is that any firm listed on the U.S. government's Entity List has been identified for restrictions on sales or transfer of U.S. technology due to a preponderance of evidence that the entity has connections to actors in the government or military in China that pose U.S. national security risks. While the Entity List would not itself restrict purchasing technology from any identified firm, the fact that any firm is listed there reflects there are factors of concern related to U.S.

national security that should be factored into any sensitive commercial or U.S. government procurement decisions.

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

Answer: Democracies with systems based on rule of law as well as non-democracies considered to be like-minded governments.

Honorable Russ Fulcher

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.

1. 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?

Answer: A Data Allies approach involves a coalition of partners (democracies with systems based on rule of law as well as non-democracies considered like-minded governments) working together within a framework to develop principles for transferring data among themselves. Allies use a principled basis to facilitate more data sharing within each other, while also using a more strict standard for "adversary" countries like Russia and China to access Americans' data. The OECD "Declaration on Government Access to Personal Data held by Private Sector Entities" announced on December 14 represents an example of this kind of approach for facilitating data flows among OECD nations. The Commerce Department's Global Cross Border Privacy Rules (CBPR) Declaration also fits into this model by promoting data flows among certain countries based on an international certification system.
This model could also take the form of an adequacy determination approach to allies, drawing on the European and UK systems.

Creating a coalition of data-sharing allies would help the United States more seamlessly import data with economic and national security benefits. Despite the emphasis in recent U.S. policy proposals on restricting outbound U.S. data transfers, the reality is that the United States primarily imports, not exports, data from the rest of the world. Since the United States is a data importing country (both from an economic and national security perspective), we benefit from policies that help create a durable coalition of countries allowing their data to be sent to the United States. The ability of U.S. firms to maintain a high rate of innovation depends upon access to global markets, talent, and, perhaps most important, datasets.

This model sets up a framework for countries to share their data—even if those countries lack identical data protection laws—by setting achievable, similar standards for data to flow. It allows more companies both large and small to operate globally, in contrast to a situation

where only a few of the largest firms can afford to comply with different data protection laws in many countries.

Being part of a large data sharing coalition, the United States could create more economic incentives for other parts of the world to join, from Latin America to parts of the Southeast Asia. The economic pull of such a coalition offers an appealing to alternative to other countries that may be considering modeling their own system based on China's model.

2. 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?

Answer: It is also important to recognize that country or geography is not synonymous with security. There are existing NIST and other internationally recognized standards for the safe and secure cloud storage practices regardless of where that data is stored.