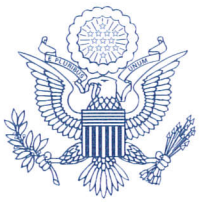
ELIOT L. ENGEL, NEW YORK
CHAIRMAN

JASON STEINBAUM
STAFF DIRECTOR

MICHAEL T. MCCAUL, TEXAS
RANKING REPUBLICAN MEMBER

BRENDAN P. SHIELDS
REPUBLICAN STAFF DIRECTOR



One Hundred Sixteenth Congress
U.S. House of Representatives
Committee on Foreign Affairs
2170 Rayburn House Office Building
Washington, DC 20515
www.foreignaffairs.house.gov

October 18, 2019

The Honorable Wilbur Ross
Secretary of Commerce
U.S. Department of Commerce
1401 Constitution Avenue NW
Washington, DC 20230

Dear Secretary Ross,

I am writing to express my deep concern about the incomplete implementation of the Export Control Reform Act of 2018 (ECRA). After more than a year, the Department of Commerce has yet to release and implement key elements of ECRA which I believe may harm our national security interests.

The emerging and foundational technology lists are a new and critical component of export control reform. Due to the pace and scale of technological innovation, many critical technologies are inadequately identified and controlled under the export control regime. The emerging and foundational technology lists were meant to help address this deficiency challenge quickly and flexibly. Your Bureau of Industry and Security had moved quickly to solicit public feedback on the composition of the emerging list by issuing an Advance Notice of Proposed Rulemaking (ANPRM) on November 19, 2018. However, almost one year later, a final emerging technology list has not been published and the timeline for completion is unclear. Moreover, the progress and timeline for the foundational list appears even more protracted.

While our regulatory process moves slowly, China is sprinting ahead to acquire critical technology by any means necessary. China's emerging regulatory regime over technology and data combined with its Civil-Military Fusion (CMF) initiative crystalize the urgency to fully implement our export control system.

China is developing a legal system that gives its government authorities the right to access any computer network operating within its administrative control. China's Cybersecurity Law, National Security Law, National Intelligence Law, Multi-Level Protection Scheme 2.0, Artificial Intelligence Program, and Social Credit System for individuals and companies are being

formulated and enforced to facilitate massive data gathering, surveillance, and control. China's Public Security Bureau has a legal right to conduct remote and on-site inspections of company networks and the authority to access and copy any data on their computer systems. The consequences for companies that store any intellectual property, know-how, or trade secret—including currently uncontrolled emerging technologies—on servers in China are significant.

Due to the structure and nature of China's political economy, any information obtained during these inspections has a heightened risk of being inappropriately shared with commercial competitors in China. As you know the Chinese government de facto or de jure owns or controls all major industries, companies, and research and development in China. Consequently, Chinese authorities have an inherent incentive—if not obligation—to share any information and data that has value with its national champions.

Compounding this inadequate protection of information and data in China is their CMF initiative. Our own Assistant Secretary of State for International Security and Nonproliferation has said the initiative, "seeks to break down all barriers between the civilian sector and China's defense industrial base in order simultaneously to achieve economic development and military modernization." In other words, if the People's Liberation Army (PLA) has identified a promising private sector emerging technology, it can take it. With the line between a commercial and military product or service blurring, concern is mounting that China may be able to acquire cutting-edge emerging and foundational U.S. technology for use by the PLA and others in China's government.

Technology is at the core of American military and economic strength. Foreign investment screenings and export controls are crucial twin pillars that help protect critical technologies from improper acquisition and use. Without an emerging and foundational technology list, the United States government has limited control and insight into what critical technology is susceptible to Chinese control.

I would appreciate if you could provide me with the following information:

- Please provide: an update on the status of the emerging and foundational list, those offices, department, and agencies involved in developing this list; and send a detailed timeline for implementation of ECRA.
- How does the U.S. government ensure engagement by the U.S. private sector with China's high-tech sector does not lead to a U.S. company supporting Chinese efforts to acquire cutting edge technology for China's armed forces?
- How does the U.S. government reconcile basic end-user commitments considering CMF and Chinese laws that give authorities the right to demand access to technology, information, and networks? And how is the U.S. government educating U.S. businesses about the potential risks associated with various collaborations with certain types of Chinese businesses?

Should you or your staff have any questions, please contact the House Foreign Affairs Committee Republican staff at (202) 226-8467, or by email at the following address: daniel.markus@mail.house.gov.

Sincerely,

Michael T. McCaul

MICHAEL T. McCAUL
Ranking Member
House Committee on Foreign Affairs

CC: The Honorable Michael R. Pompeo, Secretary of State