Statement of Richard Ashooh

House Financial Services Committee

February 7, 2023

Chairman McHenry, Ranking Member Waters, and Members of the Committee:

Thank you for the opportunity to testify before you today. Having served as Assistant Secretary of Commerce for Export Administration at the Bureau of Industry and Security (BIS) from 2017 until 2020, I had both the honor and challenge of weighing many of the issues being considered by the Committee today, especially with respect to concerns over unauthorized technology transfers. It is in that capacity that I am testifying here today.

It should be stated at the outset that the concerns at the heart of this hearing are well-founded – from the moment of my swearing in at BIS, the challenges presented by the People's Republic of China were apparent, serious, and alarming. While great strides have been made in addressing these concerns, national security and economic threats are never static and must be constantly addressed.

It is also important to stress early on that U.S. global technology leadership remains strong and that the American culture of innovation is the envy of the world. I stress this because it is essential for policy makers – as you consider the challenge of promoting U.S. technology advancement while regulating it in the face of potential threats – to cause no harm to the very thing you are trying to promote and protect. Much of what has been accomplished in recent years in this area is the result of legislation this Committee had a key role in enacting - the Export Control Reform Act and Foreign Investment Risk and Review Modernization Act, also known as ECRA and FIRRMA. There are lessons from that debate which are still relevant as Congress considers new measures such as an outbound investment regime or dramatic changes to FIRRMA or ECRA.

While the issues associated with regulating financial behaviors or technology development are many, I will confine my comments today to four recommendations that are drawn from the lessons of recent efforts to regulate in this area.

1. **Clearly define the national security threat to be addressed**. While this objective appears obvious, the temptation to address a broad panoply of legitimate concerns which do not necessarily rise to the level of a national

security threat is alluring. National security as currently understood in the United States is already very broad, taking into consideration factors such as infrastructure, supply chains, and data protection, in addition to the traditional concerns over kinetic threats. That said, a fundamental premise in national security is specificity – the concept that if everything is a threat, then nothing is. During the ECRA/FIRRMA debate, concerns over joint ventures with Chinese companies led to a robust discussion of whether to expand the scope of CFIUS to regulate this activity. Once the key issue was distilled to one of concerns over technology transfer, the purview of export controls, the appropriate tailoring of ECRA could occur. Before a new regime is established, policymakers should ensure the target of such a regime is clearly defined

2. **Regulate Horizontally.** National security threats are rarely stove-piped – solutions to address them should not be either. National security threats are commonly carried out by individuals or groups, funded by governments, with the help of – or in pursuit of – technology. Therefore, multiple agencies must collaborate – the Department of State regulates persons, Treasury the financing, and Commerce technology, with coordination from additional agencies including the Department of Defense. One of the most crucial updates to FIRRMA and ECRA – made possible by amending these statutes concurrently – was to dovetail their definitions and authorities. Establishing a unified definition of critical technologies, and grounding that definition in well-defined – and might I say well-refined – export control lists such as the Commerce Control List maintained within the Export Administration Regulations or EAR and the United States Munitions List maintained within the International Traffic in Arms Regulations or ITAR, created clear, specific, updatable tools for regulating. And since it categorizes countries and restricts them based on national security concerns, this obviated the need for Treasury to develop its own country criteria – another robustly debated issue. To the extent new concerns arise, grounding any methods to address those concerns in already existing approaches and definitions is critical This synchronization –is a model for enhancing the power and effectiveness of U.S government policy implementation.

3. **Gaps exist – leverage what works to address them.** As mentioned, the passage of ECRA and FIRRMA made tremendous improvements to both regulatory regimes and in many ways streamlined their implementation. For

all the progress made because of and since the passage of these important laws, gaps do exist in the financial space. For instance, it is currently possible that export-controlled technology could be the beneficiary of U.S. financing – intentionally or not. This disconnect is one which could be addressed through alterations to current authorities. For example, as a member of the CFIUS committee, Commerce reviews cases through the national security lens prescribed by CFIUS, but also through the overall lens of the export control system, highlighting export control implications and defense industrial base issues previously undetected. Further, the review offers Commerce the chance to vet the applicants against other important national security authorities, such as compliance with the Defense Priorities and Allocations System, making for an even more comprehensive National Security review.

In addition, a recent enhancement to the Export Administration Regulations defines the term "support" by "U.S. persons" to include, among other things, financing. While further study must be conducted, this feature of the law creates a regulatory "hook" to limit financial activities already tied to restrictions based on export controls.

One further lesson from prior deliberations bears repeating. These issues, which have the potential to staunch billions of dollars of investments, demand thorough, thoughtful review and must include public input. Input from impacted stakeholders is crucial to effective policymaking. Further, just as synchronization amongst relevant agencies and authorities is critical, high priority must be given to alignment with partner nations.

Since the passage of FIRRMA and ECRA, many like-minded countries have embarked on similar national security reviews of both foreign direct investment screening and export controls. This point merits emphasis – U.S. goals are far more impactful with a coordinated, global response. It is clear from the behavior of our allies that the U.S. has led in these areas, resulting in a more global – and therefore far more effective – approach. It should continue this leadership.

Specifically, the U.S. along with key allies should consider a new method for multilateral controls in targeted technology areas that can work with – but is separate from - the existing multilateral regime construct that has served the U.S. and partner nations well in the past, but which is ill-suited for complex technology

supply chains. The ad hoc approach as currently utilized in the area of semiconductors, for example, should be replaced with an agreed upon system among a smaller group of stakeholder nations that can act in concert, as the need arises, and with a full understanding of the nature of the technology being considered for control.

U.S. economic security is tantamount to national security and an essential driver to maintain U.S. supremacy at the leading edge. From the economic perspective, lack of multilateral or plurilateral alignment can result in ceding technology leadership through lost market leadership as industry's ability to invest the needed R&D to stay ahead becomes weakened. To continue this leadership requires that United States remain competitive in global markets and for the U.S. to move in concert with our allies.

Without such alignment, unilateral policy will ultimately fail in combating both national security and economic threats coming from China –it destabilizes U.S. leadership in the global market with foreign substitutes willing to replace U.S. companies in the supply chain and enables China to source sensitive technology and equipment in critical industries from our allies, undermining U.S. national security objectives.

U.S. global technology leadership is indisputable – but it is perishable. Hearing like this are essential to maintaining it.

I am happy to take your questions.