ide

Written Testimony of

Rob Strayer
Executive Vice President of Policy
Information Technology Industry Council (ITI)

Before the

United States Senate Committee on
Banking, Housing, and Urban Affairs

Hearing on

Examining Outbound Investment

September 29, 2022

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

Chairman Brown, Ranking Member Toomey, and Distinguished Members of the Committee, thank you for the opportunity to testify today.

My name is Rob Strayer, and I'm the Executive Vice President of Policy at the Information Technology Industry Council (ITI). I lead ITI's global policy team, driving ITI's strategy and advocacy efforts to shape technology policy around the globe to enable secure innovation, competition, and economic growth, while supporting governments efforts to achieve their public policy objectives. ITI is the premier advocate and thought leader in the United States and around the world for the information and communications technology (ICT) industry. We represent leading companies from across the ICT sector, including hardware, software, digital services, semiconductor, network equipment, cybersecurity, Internet companies, and other organizations using data and technology to evolve their businesses.

My perspective on this topic is also shaped by my time working for the U.S. government. I served as the Deputy Assistant Secretary for Cyber and International Communications and Information Policy at the U.S. State Department. In that role, I led dozens of bilateral and multilateral dialogues with foreign governments on digital economy regulatory and cybersecurity issues. I was responsible for leading the U.S. diplomatic campaign to address supply chain vulnerabilities presented by untrustworthy suppliers in foreign partners' telecommunications networks, which became an acute risk with the deployment of 5G networks. I also was involved in the interagency planning to promote trusted technology globally and to protect U.S. technology networks.

Before joining the State Department, I was the general counsel for the U.S. Senate Foreign Relations Committee and the legislative director for Senator Bob Corker, an active member of the Senate Banking Committee.

Overview

ITI appreciates the Committee holding this hearing on outbound investment screening. It is essential that the views and expertise of all stakeholders are employed to shape a new policy framework on outbound investment. As explained below, it is essential that the Congress and the Executive Branch engage in iterative consultations with the technology industry in particular to construct effective policy.

The U.S. government has no more important responsibility than to protect the nation's security. The United States should continue to pursue this commitment while staying true to the principles of free enterprise and open markets for capital investments and trade that have made the nation strong and the U.S. tech sector world leading. Our organization and the companies we represent are committed to working with Congress, the Executive Branch, and the entire stakeholder community to achieve essential national security outcomes – notably technology leadership, supply chain security, and resilience.

Importance of Technology Leadership

Companies in the United States have long spearheaded the development of the most innovative and cutting-edge technologies. These technologies have produced tremendous growth for the United States. In 2020, the U.S. information technology industry generated $1.2 trillion in domestic value added, approximately 5.5 percent of the U.S. economy; and the tech sector employed 5.9 million workers, accounting for 4.4 percent of U.S. private sector jobs.[1] These were good paying jobs with workers earning average compensation double the average U.S. private sector wage.

U.S. national security depends on continued U.S. technological leadership. This leadership drives innovation, job creation, and economic growth domestically and makes the U.S. more resilient and secure as we continue to set the pace for innovation. Transformational technologies are emerging at an accelerating rate, and the security implications of these new technologies are both more significant and more difficult to anticipate. Remaining at the cutting edge of developing and commercializing technologies will ensure they are available to the private sector and the government for a wide range of applications, including national security.

Today, other nations and their companies are competing to find the next major technological advancement. They are working harder than ever to use, exploit, and otherwise take advantage of emerging technologies to advance their own strategic, security, and economic interests. It is more important than ever that the U.S. strives to maintain its technological leadership and ensures that policy is shaped with that in mind.

How Global Technology Supply Chains and Innovation Operate

Competition in technology leadership means the market-leading technology of today will not be cutting edge tomorrow. It is a dynamic process where one generation is being improved upon by research and development (R&D) to produce the next generation. Companies use the profits earned from the sales of current products to fund R&D of the next generation. The pace of these product cycles is becoming more rapid. Some industry experts estimate that product cycles are only two to five years. This rapid innovation pace is evidenced by the Moore's Law concept of computing power on a semiconductor doubling every two years – this is because of investment in R&D. To use another example from the telecommunications sector, the time between third generation telecom technology, known as 3G, and 4G was roughly 10 years; a similar timeframe occurred between 4G and 5G. It's now estimated that 6G will arrive in about six years.

[1] Information Technology and Innovation Foundation, "How the IT Sector Powers the U.S. Economy," available at: https://itif.org/publications/2022/09/19/how-the-it-sector-powers-the-us-economy/

U.S. companies need the scale of global markets and the concomitant sales to fund the R&D to lead globally in the next generation of technology. The United States only represents 24% of global GDP. To compete with other companies that sell products and services globally, U.S. companies need access to sales in global markets and in the United States to fund the massive amounts of R&D that is necessary to be successful in the technology sector.

Aside from competition in innovation, companies face fierce competition on cost and efficiency. U.S. companies use global supply chains to access the best talent, components, and manufacturing capabilities. Mapping a supply chain is a complex task. A product or service often begins with a network of employees around the globe, each with unique talents, collaborating on design or software development. A technology product is usually based on components that originate in different locations from tiers of suppliers that are assembled into an intermediate good and then a final product, which often occurs across multiple countries. The availability and cost of inputs to a product or service will determine whether a U.S. company has a viable product in the market when competing with producers from other countries.

Taking a Comprehensive Approach to Technology Policy

ITI is very supportive of U.S. government policies ensure that leading-edge innovation continues to benefit the United States. For example, the billions of dollars in grants and tax credits in the recently enacted *CHIPS and Science Act* help companies "run faster" and better compete in the global market, and ITI was an active supporter of this legislation precisely because of its ability to support innovation in the United States. As the U.S. government considers ways to maintain its technological advantage through policies that limit outbound investments, it should seek to minimize unintended negative impacts on American technological leadership. Those impacts could be through foreclosing market access and sales that feed future R&D; and limiting the availability of key components or increasing their costs, thus harming the ability of companies to compete against global competitors who have access to those components.

With these implications in mind, I recommend that Congress and the Executive Branch consider five criteria in crafting an outbound investment regime:

1) Identify Gaps between Existing Authorities

In considering an approach to outbound investment review, it is imperative that policymakers carefully examine existing authorities, identify clear gaps in those authorities that correspond to core national security concerns, and craft new authorities in a manner that is sufficiently narrow and targeted to avoid capturing transactions already subject to existing regimes. The Executive Branch currently has several mechanisms in place to conduct national security reviews of transactions and transfers involving information and communications technologies (ICTS). Below are key examples of authorities already in place.

The U.S. Commerce Department's Bureau of Industry and Security (BIS) has extensive authority to restrict the transfer of technology, software, and commodities to countries and entities of concern. Expanding this authority, the Export Control Reform Act of 2018 (ECRA) required BIS to identify and control the export of "emerging" and "foundational" technologies, with the intent of addressing technology transfers through outbound and inbound investments.[2] Congress and the Executive Branch should ensure that this legislation has been fully and effectively implemented before developing new policy tools, including through new legislation.

By executive order, the administration also has implemented restrictions on investment in publicly traded securities of Chinese companies in the defense and surveillance technology sectors. This is known as the Chinese Military-Industrial Complex List, and it is maintained by the U.S. Treasury Department.[3]

The Secretary of Commerce also has extensive authorities to review ICTS transactions under *Executive Order 13873 on Securing the Information and Communications Technologies and Services Supply Chain* (ICTS EO). The ICTS EO grants the Secretary broad authority to review – and block or unwind -- any acquisition, importation, transfer, installation, dealing in, or use of ICTS subject to U.S. jurisdiction that involves any property in which a foreign country or national has an interest and which poses a risk to U.S. national security.[4] The Interim Final Rule ("Rule") implementing the EO captures a broad swath of ICTS transactions.[5] Based on the broad definition ICTS transactions could be interpreted to also implicate outbound investment, thus already offering the Secretary the authority to review outbound ICTS transactions. While we understand that Secretary Raimondo and this administration do not intend to use the expansive ICTS EO authorities to address national security concerns related to outbound investments, future administrations may think differently. As such, it is important to consider this existing review authority in the context of developing any new policy aimed at reviewing outbound investment transactions and ensure that they are de-duplicated or otherwise carefully aligned.

More generally, with the breadth of these existing authorities that can already be used to limit technology transfer, before adding new authorities, policymakers must identify gaps to prevent duplication and overlap, which could create a confusing landscape for both

[2] Testimony of Kevin J. Wolf, Partner Akin Gump Strauss Hauer & Feld, before the U.S. House Committee on Energy and Commerce, Subcommittee on Digital Commerce and Consumer Protection (Apr. 26, 2018), available at: https://docs.house.gov/meetings/IF/IF17/20180426/108216/HHRG-115-IF17-Wstate-WolfK-20180426.pdf.
[3] See https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list/ns-cmic-list.
[4] Securing the Information and Communications Technology and Services Supply Chain, Executive Order 13873 (issued on May 15, 2019) available at: https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain
[5] Securing the Information and Communications Technology and Services Supply Chain, Interim Final Rule; 86 FR 4909, Section 7.3 (effective date Mar. 22, 2021), available at: https://www.federalregister.gov/documents/2021/01/19/2021-01234/securing-the-information-and-communications-technology-and-services-supply-chain

government and industry. That analysis can serve as a foundation for robust public debate with stakeholders to develop effective and efficient mechanisms to address those policy gaps. If the policy goal is to reach investment activities where there is no technology or software transferred that is subject to U.S. export control restrictions, that should be explicitly articulated and the particular type of investment activities identified.

2) Identify Specific Risks to U.S. National Security

Any regulatory approach should be tied to narrow and specific national security risks. If a transaction does not implicate a specific, identifiable threat or vulnerability to U.S. supply chains or national security equities, it should not be the subject of additional regulatory reviews. A range of rationales have been suggested for outbound investment reviews, including limiting the exposure of U.S. companies' supply chains to China, preventing the Chinese military from acquiring technology, and limiting the advancement of Chinese commercial technology. U.S. policymakers should clearly define precise end goals to provide the basis for a discussion with stakeholders about how best to achieve those outcomes.

Moreover, after defining the end goals of the policy to ensure an effective regime, which as National Security Advisor Jake Sullivan put it, continues "American technological dynamism and innovation,"[6] the U.S. government should identify a narrow and specific set of transactions. That could be in the form of a limited subset of technological capabilities along with the types of transactions and ownership limitations.

The identification of particular technologies and transactions should be based on assessments by the U.S. Intelligence Community and technology experts from industry, academia, and other parts of the government. These assessments should seek to scan the horizon of emerging technologies that may have impacts on U.S. national security interests. Important questions need to be considered such as whether the technology is transformative, its impact on economic growth, national security, military capabilities, and the ability of an adversary to monopolize access to it. Recently, efforts have begun in the IC and the Commerce Department to expand economic and technological analytic capabilities. Those need to be better developed to inform the policymaking in this area.

There are several lessons from the implementation of the 2019 ICTS EO that are applicable here. The 2019 EO required the Director of National Intelligence to prepare reports on an annual basis regarding threats to ICTS, which could then be used to inform actions undertaken pursuant to that EO. However, we have never seen a public reference to such reports nor have we been made aware of any annual updates. While it is possible these reports are only in a classified format, it would be useful to know whether they have actually been completed, as they could help to inform future policymaking activity. The Secretary of Homeland Security

[6] Remarks by National Security Advisor Jake Sullivan at the Special Competitive Studies Project Global Emerging Technologies Summit on Sept. 16, 2022.

was also directed by the EO to produce an analysis of ICTS vulnerabilities with greatest consequences. While the Department of Homeland Security did produce a "criticality assessment", it focused only on a subset of the vast ICTS ecosystem – specifically, on the "connect" function of the National Critical Functions developed by CISA's National Risk Management Center.

The breadth of information and communications technologies and services implicated under the ICTS EO means that the U.S. government must focus future restrictions. However, to date we have not seen the Secretary take steps to exercise the authority granted under that EO and associated rulemaking to review, prohibit, and unwind transactions. A new executive order that authorizes reviews of outbound investment transactions, potentially in all sectors of the economy including ICTS, would similarly need to be narrow in application to make its enforcement manageable and to mitigate unintended adverse consequences for U.S. businesses and capital markets. That narrow and ideally iterative process of scoping an outbound investment framework should be based on an assessment by the IC, other parts of the U.S. government, and relevant stakeholders. The analysis should take place ***before*** such a regime enters into force.

3) Consult with Industry Iteratively

U.S. policymakers should consult with the technology industry as part of a structured process when shaping outbound investment review policies. The private sector has the best data and understanding of supply chains. It can share this understanding with the government to design policies that achieve the goals the U.S. government seeks, while minimizing costs to supply chains, innovation, and global competitive positioning for U.S. companies. Such consultations should occur both with respect to technologies covered and the types of investment transactions. This should not be a one-time consultation, but done iteratively as the government proceeds incrementally with restrictions and seeks to refine policies. The U.S. government should establish an advisory board with senior U.S. government leadership and private sector executives that would make recommendations about technology that should be designated for outbound investment restrictions. ITI hopes that this is one of many opportunities to engage with the U.S. government about outbound investment screening.

4) Develop Clear Lines and Avoid Ambiguity

The private sector will support and adhere to regulatory direction provided by the U.S. government designed to protect national security. To minimize the impact on business competitiveness, companies need as much certainty as possible to plan their supply chains, which in most cases take years to develop. The best way to provide that certainty is with clear lines about the investments that would be covered by regulatory restrictions. In an internationally competitive investment environment, a U.S. company could lose out to a foreign competitor seeking to make the same acquisition if the U.S. company must condition the transaction on government regulatory review that may take many months or years.

However a review regime is constructed, it should avoid ambiguity that may chill a broader range of investments and hurt the competitiveness of U.S. companies.

5) Seek to Build International Coalitions

It is critically important that new regulatory mechanisms be coordinated with U.S. allies and partners to ensure any proposed reforms minimize the likelihood that unilateral U.S. actions will incentivize investment to leave the United States and be made from countries that do not have the restrictions imposed by the United States. We should not undermine U.S. competitiveness and technological leadership by making our allies and adversaries potentially more attractive destinations for investment.

To achieve this coordination, it is essential the U.S. government articulate its goals and objective criteria for the review of investments. The U.S. government's experience educating partners about the risk from untrustworthy 5G telecommunications suppliers should be instructive. The government was asked about the risks to telecom networks and why particular suppliers presented increased risks. Rather than only presenting bottom-line conclusions about the exclusion of untrustworthy suppliers from U.S. networks, the U.S. government provided objective criteria that those countries could apply and helped them reach similar conclusions about network risks form those suppliers. Similar coordination based on objective, articulable criteria will help generate aligned approaches to international investment restrictions and avoid making the U.S. less competitive.

Conclusion

The U.S. government should take a comprehensive approach to understanding the complexity and challenges of outbound investment screening to ensure an effective regime to protect national security and American technological leadership. Technology companies rely on global supply chains to bring products to market and need the sales of global markets to fund R&D and further innovations. They face competition from companies in both allied and adversary countries that will continue to have access to markets that could be restricted for U.S. companies by outbound investment screening, unless these efforts are taken in concert with allies and global partners.

Policymakers should identify the gaps in current authorities that restrict the transfer of technology and articulate the specific goals for a new authority involving investments. When that authority is employed, it is important for the U.S. government to apply objective clearly defined rules to a narrow range of technologies and transactions. The private sector has the best information about supply chains and the development of transformative innovations so it should be consulted with regularly in scoping the policy. It is important for there to be coordination among other governments to implement the same restrictions, so that U.S. companies are not disadvantaged in global markets.