

EXAMINING OUTBOUND INVESTMENT

HEARING
BEFORE THE
COMMITTEE ON
BANKING, HOUSING, AND URBAN AFFAIRS
UNITED STATES SENATE
ONE HUNDRED SEVENTEENTH CONGRESS
SECOND SESSION
ON
EXAMINING CURRENT ISSUES RELATED TO OUTBOUND U.S. INVEST-
MENT AND WHETHER THERE ARE GAPS IN EXISTING AUTHORITIES
THAT PRESENT NATIONAL SECURITY RISKS TO THE UNITED STATES

SEPTEMBER 29, 2022

Printed for the use of the Committee on Banking, Housing, and Urban Affairs



Available at: <https://www.govinfo.gov/>

U.S. GOVERNMENT PUBLISHING OFFICE

53-682 PDF

WASHINGTON : 2023

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

SHERROD BROWN, Ohio, *Chairman*

JACK REED, Rhode Island	PATRICK J. TOOMEY, Pennsylvania
ROBERT MENENDEZ, New Jersey	RICHARD C. SHELBY, Alabama
JON TESTER, Montana	MIKE CRAPO, Idaho
MARK R. WARNER, Virginia	TIM SCOTT, South Carolina
ELIZABETH WARREN, Massachusetts	MIKE ROUNDS, South Dakota
CHRIS VAN HOLLEN, Maryland	THOM TILLIS, North Carolina
CATHERINE CORTEZ MASTO, Nevada	JOHN KENNEDY, Louisiana
TINA SMITH, Minnesota	BILL HAGERTY, Tennessee
KYRSTEN SINEMA, Arizona	CYNTHIA LUMMIS, Wyoming
JON OSSOFF, Georgia	JERRY MORAN, Kansas
RAPHAEL WARNOCK, Georgia	KEVIN CRAMER, North Dakota
	STEVE DAINES, Montana

LAURA SWANSON, *Staff Director*

BRAD GRANTZ, *Republican Staff Director*

ELISHA TUKU, *Chief Counsel*

DAN SULLIVAN, *Republican Chief Counsel*

CAMERON RICKER, *Chief Clerk*

SHELVIN SIMMONS, *IT Director*

PAT LALLY, *Hearing Clerk*

C O N T E N T S

THURSDAY, SEPTEMBER 29, 2022

	Page
Opening statement of Chairman Brown	1
Prepared statement	30
Opening statements, comments, or prepared statements of:	
Senator Toomey	3
Prepared statement	31

WITNESSES

Senator Robert P. Casey, Jr., of Pennsylvania	5
Prepared statement	32
Senator John Cornyn of Texas	7
Prepared statement	35
Sarah Bauerle Danzman, Associate Professor of International Studies, Indiana University	10
Prepared statement	36
Responses to written questions of:	
Senator Sinema	53
Richard Ashooh, Former Assistant Secretary for Export Administration, U.S. Department of Commerce	11
Prepared statement	44
Responses to written questions of:	
Senator Sinema	53
Thomas Feddo, Former Assistant Secretary for Investment Security, U.S. Department of the Treasury	13
Prepared statement	46
Responses to written questions of:	
Senator Sinema	53
Robert Strayer, Executive Vice President of Policy, Information Technology Industry Council	15
Prepared statement	48
Responses to written questions of:	
Senator Sinema	54

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

Statement submitted by the AFL-CIO	55
Statement submitted by Representative Rosa L. DeLauro of Connecticut and Representative Bill Pascrell, Jr., of New Jersey	57
Statement submitted by BSA / The Software Alliance	58

EXAMINING OUTBOUND INVESTMENT

THURSDAY, SEPTEMBER 29, 2022

U.S. SENATE,
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS,
Washington, DC.

The Committee met at 10 a.m., via Webex and in room 538, Dirksen Senate Office Building, Hon. Sherrod Brown, Chairman of the Committee, presiding.

OPENING STATEMENT OF CHAIRMAN SHERROD BROWN

Chairman BROWN. The Committee on Banking, Housing, and Urban Affairs will come to order. Good to see my two colleagues here. I will introduce them in a moment. I will begin with opening statements, as the Ranking Member, Senator Toomey, will too.

Today's hearing, as many of ours always are, I believe every case, is a hybrid format. Witnesses, both two colleagues and the other witnesses, are in person, but Members have the option to appear in person or virtually.

Earlier this year Secretary of State Antony Blinken said that "Beijing wants to put itself at the center of global innovation and manufacturing, increase other countries' technological dependence, and then use that dependence to impose its foreign policy preference. And Beijing is going to great lengths to win this contest," unquote.

It is critical that the Administration has the tools it needs to protect our national security. This Committee has played a key role. We have done that through export controls that restrict the flow of sensitive technology, and we have done that through the screening of foreign direct investment into the U.S., to guard against adversaries accessing our technology or critical infrastructure capabilities.

Four years ago, we enacted the Export Control Reform Act, ECRA, which provided permanent statutory authority for the U.S. Government to regulate U.S. exports that have commercial and defense applications.

Those controls can apply to important technology, like semiconductors. They can apply to the way a technology is used, like military intelligence, and they can apply to who uses it, like a Chinese quantum computing company.

Along with ECRA, we also passed the Foreign Investment Risk Review Modernization Act, known as FIRREA. That law strengthened and expanded the jurisdiction of CFIUS, and Senator Cornyn especially worked on that issue, that reviews foreign investments, like mergers or acquisitions, of U.S. businesses. We passed these

bipartisan laws because we all recognize the importance of maintaining U.S. technological leadership, and the need to protect that leadership.

We know that threats to our national security are evolving. We also know that our adversaries will use any means they can to close the gaps between our technological capabilities and theirs, without much care to how legal their tactics actually are. What we do not know is to what degree U.S. investments are helping them close those gaps.

U.S. investments—a venture capitalist or pension fund—could wittingly or unwittingly support foreign technological investments that, in the words of our Secretary of State, could, quote, “increase other countries’ technological dependence, and then use that dependence to impose its foreign policy preference.”

We cannot let that happen. It is why policymakers have been examining the role that U.S. investments abroad are playing to enable foreign adversaries, as they develop technologies that could take away our technological edge and damage our national security.

Senators Casey and Cornyn introduced a bill designed to address these concerns by requiring notifications of certain investments, and enabling the President to prohibit others. I thank them for that introduction.

Without objection, I would like to enter into the record letters of support for that bill, the first from Representatives DeLauro and Pascrell, who introduced companion legislation in the House, and the second from the AFL–CIO, which supports that legislation. Without objection, so ordered.

Chairman BROWN. We need to better understand whether U.S. investments abroad pose national security risks. In a global economy where capital flows freely, we need to ensure that we are not investing in technologies that harm our national security.

Prior to creating CFIUS, we had not systematically tracked foreign investments into the United States. Times change, and so do the threats we face. We must understand the scope of outbound investment and address the impact it plays in supporting efforts by our adversaries to achieve their “foreign policy preferences.”

Protecting U.S. technological leadership is an important part of this conversation, and it is why we are here today. But it is also not the whole story. And I talked with Senator Casey about this privately over the years, many times. The story is an issue that Ohioans and Pennsylvanians, especially the industrial Midwest, know well.

Over the last 30 or 40 years, corporations searched the globe for cheap labor. First they went to anti-union States, shutting down in Pittsburgh or Cleveland and moving production to Mississippi or Alabama. Then corporations lobbied for tax breaks and bad trade deals to help move jobs overseas, always in search of lower wages. They started with manufacturing jobs, but they did not stop there. Corporations, in some cases, moved R&D jobs abroad too.

And Wall Street rewarded them over and over and over.

In some cases, investments abroad outpaced investments in American workers, undermining our national security and in so

many communities in the industrial Midwest but really all over the country, hollowed out our middle class.

Protecting technological leadership and protecting jobs are connected. Ohioans know how much innovation happens on the shop floor.

Investing in our workers, our infrastructure, our educational system, and our research, development, and manufacturing will help shore up supply chains.

From the Infrastructure bill to the CHIPS and Science Act to the Inflation Reduction Act, this Congress is laying down a new marker: the technology of the future, from semiconductors to batteries to electric vehicles, will be developed in America and made in America, by American workers.

It has not been easy, and our work is far from finished, but I am optimistic.

I look forward to working with the Administration and my colleagues on this crucial issue for our economy.

Senator Toomey.

OPENING STATEMENT OF SENATOR PATRICK J. TOOMEY

Senator TOOMEY. Thank you, Mr. Chairman. Welcome to my colleagues.

China's economic and military rise poses the greatest challenge to core U.S. interests since the end of the cold war. Under Xi Jinping's autocratic rule, China is seeking to dominate the Indo-Pacific, with clear security implications for U.S. allies and partners there, and they are engaging in relentless efforts to undermine human rights and American values, including free expression, the rule of law, and democratic governance.

Recently, White House officials and a few of my Senate colleagues have advanced a peculiar idea that in order to fully meet this challenge posed by China the United States should adopt some of the Chinese Government's strategies for managing its economy. That thinking has led this Congress to enact industrial policy like new distortive taxpayer subsidies for semiconductor manufacturing. I thought that approach was a big mistake.

Especially given that recent episode, I am concerned about efforts to impose new capital controls on American investment in China. Advocates want a new regulatory regime so U.S. officials are notified of, and can potentially stop, U.S. investments in certain Chinese businesses. If those investments credibly pose a risk to our national security, then I am not reflexively opposed to this concept.

However, there are several reasons why we should proceed very carefully with this idea.

Some claim that current U.S. legal authorities, including our dual-use Export Control System overseen by the Bureau of Industry and Security, or BIS, are inadequate or incapable of addressing the risk posed by American investments in China. But it is important to remember that BIS regulates the flow of goods, software, and technology into jurisdictions and to end users of concern, including China, and retains the force of law in the context of a U.S. investment.

As Commerce Undersecretary Alan Estevez told this Committee in July, BIS has complete authority to block the transfer of any

kind, of technology, intellectual property, blueprints, procedural know-how, or software going to China, including when made in the context of an American investment in China. What, then, is the need for an outbound investment notification regime?

Well, in the words of National Security Advisor Jake Sullivan, it would capture outbound investments that, and I quote, “circumvent the spirit of export controls,” end quote. It appears Mr. Sullivan was referring to certain U.S. investments in China that are legal under U.S. law, but might be, nevertheless, of concern.

It appears that Mr. Sullivan’s concern is investments that could result in the transfer of operational and managerial expertise and enhance the ability of Chinese firms to make sophisticated technologies might be prohibited from receiving if a U.S. company wanted to export those technologies. The inherent problem with Mr. Sullivan’s invoking the “spirit of export controls” is it is hard to define a “spirit,” and therefore, it could be subject to expansive and varying interpretation.

I think we should carefully examine this issue. I am concerned that the White House is reportedly rushing to issue an Executive order that establishes an outbound investment regime unilaterally. Let me be very, very clear about this. An Executive order is not a substitute for a new congressionally passed law. Legislation benefits from a deliberative, open, accountable democratic process.

A White House EO will inherently lack these characteristics, even if an EO is accompanied by a notice and comment period, and certainly it should not precede a law. In addition, an EO will, it is my understanding, very likely place no limits on what technologies can be added to the regime in the future.

Why is it important to establish clear parameters on an outbound regime from the outset? Because time and again, Presidents of both parties have misused sweeping national security authorities in ways far beyond how Congress initially intended. President Trump nearly used IEEPA to impose tariffs on Mexico over immigration policy, and Democrat and Republican senators were shocked when President Trump abused Section 232 “national security” authority to impose tariffs on U.S. partners and our closest allies. And frankly, we should all be equally opposed to the Biden administration’s continuation of the Trump administration’s abuse of power under Section 232, which continues to this day.

Appropriately scoping an outbound regime is very, very important to preclude it from being used as a back door for trade protectionism in the future.

It is absolutely vital that we prevail in this contest with China. We can do so by ensuring that the United States remains the single greatest global destination for capital formation, research and development, and the smartest minds in the world to come and work.

Creating a flawed outbound investment regime would undermine our economic leadership, discouraging the flow of capital, ideas, and people into the United States. After all, why would you start a firm in the U.S. if you know doing so risks precluding you from investing in China, the second largest economy in the world?

Given these stakes, I am recommending a set of principles to guide the creation of any outbound investment regime. These prin-

ciples are based on the premise that it would be wholly irresponsible to have a regime that does not have clear statutory boundaries on its application. Therefore, a notification regime for outbound American investments in China should, at a maximum, only be applicable to direct U.S. investments in Chinese entities that are manufacturing, producing, developing, or testing a technology for which a U.S. exporter would otherwise be required to seek a license under current U.S. law to export. I intend to solicit feedback on these principles, and I would like very much to work with Senators Cornyn, Casey, and Chairman Brown to incorporate them into the upcoming National Defense Authorization Act.

Thank you, Mr. Chairman.

Chairman BROWN. Thank you, Senator Toomey.

Today the Committee has the honor of welcoming Senator Casey of Pennsylvania, who came to the Senate in 2007, and Senator Cornyn of Texas, who came 2 years earlier. When I joined this Committee in 2007, Senator Casey and I sat down at the end of the dais. You could barely see the Chairman's chair from there, and his has always been a critical voice for workers in the Senate.

Welcome back, Bob.

We also welcome back Senator Cornyn. It was just 5 years ago this month that Senator Cornyn testified before this Committee on legislation to reform and strengthen our outbound investment review process. Thank you for that work. Today we hear from them about the need for outbound investment screening and about their proposals.

Senator Casey, proceed. Thank you.

STATEMENT OF SENATOR ROBERT P. CASEY, JR., OF PENNSYLVANIA

Senator CASEY. Chairman Brown, thank you very much, and Ranking Member Toomey and Members of the Committee, I want to thank you for this opportunity to testify in support of an outbound investment screening mechanism.

I am grateful that Senator Cornyn is here with us today and for his ongoing partnership on this effort, as well as our colleagues in both the House and the Senate who are sponsors of the legislation, the National Critical Capabilities Defense Act, Senate Bill 1854, including, in the House version of this legislation Representatives DeLauro, Pascrell, Fitzpatrick, and Spartz.

For decades, the United States has steadily ceded its manufacturing power to other countries, particularly foreign adversaries, like the People's Republic of China. Outsourcing our manufacturing and supply chains has put our economic and national security at risk. The pandemic exacerbated this problem, as we experienced shortages of PPE and computer chips simply because we were reliant on other countries to manufacture them and a broken supply chain to get them to us.

In 2020, during the pandemic, I first introduced the National Critical Capabilities Defense Act to require targeted Government screening of certain transactions by U.S. companies doing business in adversarial countries. This bill would help the U.S. better understand the risks of relying on foreign adversaries to design and

manufacture goods critical to our economic and national security interests.

Our goal must be—it must be to safeguard critical domestic industries and capabilities for American workers, manufacturers, and innovators. We must avoid any action that aids or abets our adversaries.

Manufacturing, as we all know, is the foundation of our economic competitiveness. Working men and women in Pennsylvania, for example, have seen the damage of decades of offshoring and the hollowing out of American manufacturing strength and the knowledge that goes with it, what that does to communities and those industries.

According to the Economic Policy Institute, the People's Republic of China cost the U.S. 3.7 million jobs between 2001 and 2018—2.8 million of those jobs, three-fourths of the total, were in manufacturing. In Pennsylvania, 137,300 of those jobs were our manufacturing jobs. But job numbers alone provide little insight into the family and community trauma, as well as the economic scarring that have ravaged many small towns in Pennsylvania and other States. In key sectors such as communications equipment, electronics, and computer technology, we have ceded up to 40 to 60 percent of the domestic market share to Chinese imports.

As U.S. firms continue to invest in high-tech and advanced services sectors, many of these investments have been made in countries that are owned, controlled, or influenced by the Chinese Communist Party.

As of 2020, U.S. investments in Chinese companies totaled, in terms of capital investment, \$152 billion to Chinese State-owned enterprises, \$54 billion to Chinese military companies. At present, the U.S. has little knowledge of where these dollars are going and what sort of projects they may be supporting.

We risk funding threats to our own national security. According to former U.S. National Security Adviser H.R. McMaster, venture capital firms are pouring billions into Chinese companies that are, quote, “developing dual-use and sensitive technologies that are going to be weaponized against us or already are aiding and abetting the Russians,” unquote. Without a mechanism or a process to understand the ways in which the export of U.S. investments and capabilities are resulting in a wholesale transfer of American R&D and expertise to our adversaries, without that the U.S. is an active party in the decline of our own economic might and national security.

The Chinese Communist Party has made clear its willingness to sever access to critical supply chains and use economic coercion to bully other Nations. I will not give you examples of that. There are many in Australia and Lithuania and so many others.

So I believe we have to confront a Chinese regime that is determined to cheat and bully its way to economic superiority. Some critics have said that outbound investment screening is something that should be left to the free market and private companies to sort out. Our adversaries, as we all know, will violate international law and they will ignore both private enterprise itself and free market rules.

The People's Republic of China and its broader military and governmental ambitions are intertwined with its trade and economic actions because the Chinese Government's agenda blurs the lines between its economic and defense sectors by way of its "civil-military fusion." When Chinese firms and State-owned enterprises compete against America's, it is done so with broader objectives in mind, including those of their military.

It is up to U.S. policymakers, not international markets, to be vigilant regarding our national security, our manufacturing capacity, and the protection of our workers.

There are significant gaps that exist in our export control programs and existing authorities. The U.S. should align our own outbound investment review mechanism with those of allies and partners such as South Korea and Taiwan, who have already taken the necessary steps to protect their national security.

So I want to thank so many others who have worked on this, in addition to Senator Cornyn, as I mentioned, and thank the Administration for its support. And with that, being a little bit more than a minute over, I will conclude my remarks. Mr. Chairman and Mr. Ranking Member, thank you for the time.

Chairman BROWN. Thank you, Senator Casey.

Senator Cornyn is recognized. John, welcome.

STATEMENT OF SENATOR JOHN CORNYN OF TEXAS

Senator CORNYN. Thank you very much, Mr. Chairman, Ranking Member Toomey for scheduling this hearing on a very important topic. The Chairman's comments about the reforms we made to the Committee on Foreign Investment in the United States 5 years ago—it is amazing how quickly time flies—which have now been modeled by other countries, other democracies around the world because of the awareness of the threat of some foreign investment technology transfers and the like posed to not only those democracies' economies but also to their national security.

I am pleased to be here with my friend, Senator Bob Casey. It is no coincidence that we are both members of the Senate Select Committee on Intelligence. We get regular reports, some we cannot talk about here, about what our adversary, the People's Republic of China, is doing. But I think the contours are pretty well-known in the open record.

Deng Xiaoping opened up the Chinese economy recognizing the only way they were going to be able to grow their economy was by soliciting foreign investment to that country from the United States, and they did a magnificent job. They are, as I think Senator Toomey mentioned, the second-largest economy in the world and growing still, although they do have serious challenges, both economic and from a demographic standpoint.

But there is no question that China poses a threat to our national security. We had hoped that they would join the liberal rules-based order, particularly when they were admitted to the World Trade Organization, but those hopes and wishes have certainly been dashed by the hard reality that Senator Casey mentioned a moment ago. It did not take long for the openness that we hoped would follow, was abused by the Chinese Communist Party through outright theft and control.

And now we are seeing the vulnerabilities of an open door between our economies. The Chinese Communist Party has weaponized our trade and financial apparatuses and is using them to achieve control, dominance, and self-sufficiency in the area of our national critical capabilities. “Made in China 2025” is just one example of that. And, of course, they resort to all sorts of illicit means to secure access to not only our intellectual property but also the know-how that makes it more likely that they will achieve that goal.

But as we look at technologies such as semiconductors, quantum computing, and artificial intelligence, which are high on the list of priorities for the Senate Select

Committee on Intelligence, the U.S. is the only allied Pacific Nation that provides domestic semiconductor incentives and does not have an outbound investment mechanism.

The CCP’s predatory trade practices paint an alarming picture for our national security, which requires a whole-of-Government response as well as that by American businesses, our friends and allies around the world, and those Nations who at least attempt to abide by the rules-based international trading system.

That said, to the point made by the Ranking Member, my friend, Senator Toomey, we must not overreach. Trade and investment with China must continue, and it will continue, so any legislative or regulatory actions must be targeted. And I prefer whichever comes first. We need the scalpel, not the sword.

The first step is to improve visibility into the human, financial, and intellectual capital in foreign adversary Nations. We must know the full extent of the problem.

Recently we had an open hearing of the Intelligence Committee where one witness testified that the market value of American investments in the People’s Republic of China was \$2.3 trillion. American businesses literally funded the rise of the People’s Republic of China. And no one is suggesting that we decouple entirely, but we do need to look at this with our eyes wide open.

I know a robust process that focuses on transparency and notification is the best answer. The American people should know if a company is investing in critical industries on a foreign adversary’s soil. And as you know, there is no real firewall between the People’s Liberation Army and private businesses. Businesses in China are compelled to share critical information with the People’s Liberation Army that could be used for military purposes as well.

And of course, in the event of a conflict with Taiwan or worse, our own men and women in uniform, would be at a disadvantage to a Chinese military that was funded in part by an American company.

I would like to note that this is not just a hypothetical. This happened. That is why this is so critical.

There is an old saying attributed to Vladimir Lenin. “The capitalists will sell us the rope with which we will hang them.” That is exactly what China is trying to do—using the enterprising minds of America to choke our economy.

The challenge we face with regards to China in particular requires a shift in our way of thinking, a new paradigm. This is not the China that Richard Nixon visited many years ago. The focus

on proxy wars and diplomacy are a relic of the past. We need real action.

That said, our Government cannot risk playing politics with an important topic like outbound investment to settle centuries-old debates over protectionism versus free trade or labor versus big corporations. But I know we need to act soon. I agree with Senator Toomey that legislative action is far preferable to Executive orders, for a variety of reasons that we do not need to go into here. But I know that the Administration, in my conversations with Secretary Raimondo in particular, they would welcome congressional action, and I think taking that initiative is very important, which is what Senator Casey and I have been trying to do for quite some time now.

The perspectives of this panel are very important, and I again welcome the continued conversation as we work our way to hopefully a negotiated outcome. I like the idea suggested by Senator Toomey that maybe this would be a candidate for inclusion in the National Defense Authorization Act.

But let me just say again my thanks to Senator Casey for his leadership and for being such a productive partner.

I appreciate the work of this Committee on this topic, as I do the work that we have done in the past together on things like CFIUS. And I hope it is one of several hearings to come that will provide additional and diverse perspectives and oversight on this topic.

Thank you very much.

Chairman BROWN. Thank you, Senator Cornyn and Senator Casey. I know you both have busy schedules. That is my nice way of saying you are dismissed and we need to have the witnesses sit there, so thank you for joining us and your thoughtful testimony.

I will introduce the second panel as they arrive.

Sarah Bauerle Danzman is an Associate Professor of International Studies at Indiana University and a nonresident senior fellow at the Atlantic Council. Previously she was at the Council on Foreign Relations, working on the Office of Investment Affairs at the State Department. Welcome, Ms. Bauerle Danzman.

The Honorable Richard Ashooh is the Former Assistant Secretary for Commerce for Export Administration, currently Vice President of Global Government Affairs for Lam Research Corporation. Welcome, Mr. Ashooh.

The Honorable Thomas Feddo, former Assistant Secretary of the Treasury for Investment Security after FIRREA created the position, leading the Committee on Foreign Investment in the U.S. Presently he is the founder of The Rubicon Advisors. Welcome, Mr. Feddo.

And last, joined by an Ohioan and Dennison University graduate, where my father and brother went, Mr. Robert Strayer. He served as Deputy Assistant Secretary for Cyber and International Communications Information Policy at the State Department. He is now the Executive Vice President of Policy, Information Technology Industry Council.

Thank you all for joining us, and Ms. Bauerle Danzman, please proceed. Thank you.

STATEMENT OF SARAH BAUERLE DANZMAN, ASSOCIATE PROFESSOR OF INTERNATIONAL STUDIES, INDIANA UNIVERSITY

Ms. BAUERLE DANZMAN. Thank you, Chairman Brown, and Ranking Member Toomey, as well as your hard-working staffs for inviting me to testify on outbound investment. It truly is an honor to speak with the Committee today.

I am an Associate Professor of International Studies at the Hamilton Lugar School at Indiana University where I study the intersection of national security and investment policy. As a Council on Foreign Relations International Affairs Fellow, I worked as a policy advisor and CFIUS staffer in the Office of Investment Affairs at the Department of State in 2019 and 2020.

And as a Fellow at the Atlantic Council I have had the distinct pleasure of coleading a policy working group on outbound investment controls with Emily Kilcrease of the Center for New American Security. Emily and I recently published a policy brief where we lay out our suggestions for how to design an appropriately scoped outbound screening mechanism. Much of my comments today draw directly from that coauthored report.

I want to spend my time offering five observations that Congress should keep in mind while contemplating outbound investment controls.

First, there are some actual real gaps in the United States' ability to address national security risks associated with some kinds of outbound investment. Export controls can stop the flow of U.S. technology to these activities, but active forms of U.S. investment, particularly foreign direct investment and venture capital, can provide intangible benefits to the Chinese firms and industries in which they invest, and we do not currently have controls on that.

Second, Congress should resist temptations to use outbound investment screening for purposes other than national security. To be consistent with a longstanding commitment to open markets, the authority to intervene in an outbound transaction must be limited to a fact-based national security risk assessment, as is the case with inbound investment through the CFIUS process. It is my assessment that any outbound screen should focus on the national security risks associated with indigenous technology development in countries of concern.

Third, Congress should recognize the uncertainty that pervades this issue. Current data collection on U.S. investment flows to China are not detailed enough to be able to assess the national security implications of individuals transactions. A notification regime could help to scope the size of the problem and is an important first step.

An Executive order related to outbound screening may be a good first step because it would also allow for more experimentation before committing to a statutory requirement. This mirrors the experience of CFIUS, which was first established through Executive order in 1975, and only gradually became a statutory requirement through a series of amendments to the Defense Production Act.

Fourth, Congress should not assume that a mirror image of CFIUS will work for outbound screening. The enforcement issues associated with regulating the movement of investment abroad is more challenging to address than regulating inbound flows. Con-

gress should only move forward with a screening concept if it is reasonably sure that it has adequate monitoring and enforcement capabilities to give the regulation teeth.

And finally, Congress should think in network terms when contemplating which technologies a screening regime should cover. An administrable outbound investment review system will need to be relatively narrow in scope. We should avoid a boiling-the-ocean mentality. A broadly scoped review is likely to generate substantial negative consequences for U.S. companies' competitiveness and capacity to innovate. Congress can narrow its focus while remaining maximally effective by examining technology checkpoints and supply chain networks, where U.S. firms currently have the advantage and where process and knowhow are central to the production of these technologies.

Technologies for which China has the least domestic capacity tend to be in areas with very high-quality control specifications. These kinds of technologies are likely of high national security value, require substantial knowhow to perfect, and have outsized follow-on effects to other technologies relevant to U.S. national security. Those would be good candidates for review.

However, we should be wary of overreach. Prudent policy must balance the national security imperative to deny countries of concern indigenous capabilities in technologies of high national security import while also avoiding an overly restrictive regime that would actually inadvertently further push Chinese entities toward self-sufficiency.

Thank you for the opportunity to speak with you today, and I look forward to your questions.

Chairman BROWN. Thank you, Ms. Bauerle Danzman.

Mr. Ashooh, welcome.

STATEMENT OF RICHARD ASHOOH, FORMER ASSISTANT SECRETARY FOR EXPORT ADMINISTRATION, U.S. DEPARTMENT OF COMMERCE

Mr. ASHOOH. Thank you, Mr. Chairman. It is good to be with you and also with you, Ranking Member Toomey. It is an honor to be here today.

Having served as Assistant Secretary at BIS I contend with many of the issues which are the subject of today's hearing, and I certainly share the concerns that were stated in both of your statements. And it is in that capacity, my experience at BIS, that I would like to testify today and share with you.

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 PRC were apparent, serious, and alarming. While great strides have been made in addressing these concerns, national security is never static and must be constantly addressed.

Much of what has been accomplished is the result of legislation this Committee championed, as has already been mentioned, in 2018, which led to the Export Control Reform Act and Foreign Investment Risk and Review Modernization Act, also known as ECRA and FIRRMA.

And I would like to take a minute to underscore my gratitude to the Committee for the thoughtful approach it took at that time,

which involved bipartisan, bicameral, and multijurisdictional legislating to advance a long-overdue modernization of some very complex and powerful authorities. Any consideration of measures which could significantly alter U.S. capital flows merits a similarly thoughtful and thorough approach.

I will confine my comments today to three recommendations that are drawn from the lessons learned in the implementation and passage of FIRRMA and ECRA.

First, clearly define the national security threat to be addressed. While this objective appears obvious, the temptation to address a broad panoply of otherwise legitimate concerns that do not necessarily meet the test of national security is very alluring.

However, a fundamental premise in national security specificity during the ECRA and FIRRMA debate, concerns over joint ventures with Chinese companies, led to a robust discussion of whether to expand the scope of CFIUS to regulate that 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, thanks in large part to the concomitant updating of that law along with FIRRMA.

Second, I recommend in this area that we regulate horizontally. National security threats are rarely stove-piped, and solutions to address them should not be either. Multiple agencies must collaborate—the Department of State regulates persons, Treasury the financing, and Commerce the technology.

One of the most crucial updates in FIRRMA and ECRA was to dovetail their respective definitions and authorities, which established a unified definition of critical technologies, which grounded that definition in well-defined export restriction criteria such as the Commerce Control List and the United States Munitions List under ITAR. This created clear, specific, updatable tools for regulating. And since the Commerce List 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 at that time. This synchronization is a model for enhancing the power and effectiveness of U.S. policy implementation.

Third, I recommend building on what works. For all the progress made because of and since the passage of FIRRMA and ECRA, gaps do exist. As has already been mentioned, it is possible that export control 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. ECRA and FIRRMA allowed the two regimes to reinforce each other as complementary tools to protect national security. As a CFIUS-reviewing agency, commerce has the opportunity to vet applicants against other important national security authorities such as compliance with Export Control System and the Defense Priorities and Allocations System, also known as DPAS, making for an even more comprehensive national security review.

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.

Amendments to current authorities hold the potential to address the most pressing concerns regarding outbound investments without, as has been proposed, the establishment of an additional, entirely new regime with potentially overlapping or conflicting authorities.

Finally, just as alignment among relevant agencies and authorities is critical, consideration 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. It is clear from the behavior of our allies that the U.S. led in these areas, resulting in a more global, and therefore far more effective, approach. It should continue this leadership in this area.

And I am happy to take your questions.

Chairman BROWN. Thank you very much, Mr. Ashooh.

Mr. Feddo, welcome. Thank you for joining us.

STATEMENT OF THOMAS FEDDO, FORMER ASSISTANT SECRETARY FOR INVESTMENT SECURITY, U.S. DEPARTMENT OF THE TREASURY

Mr. FEDDO. Thank you, Chairman Brown, Ranking Member Toomey, and distinguished Members of the Committee. When I last appeared before you I was fortunate to receive your endorsement to be the Treasury Department’s first-ever Assistant Secretary for Investment Security. In that role,

I oversaw the Committee on Foreign Investment in the United States, including the successful implementation of FIRRMA in 2018.

By virtue of that experience and over 20 years of service in national security-related capacities, I hope to contribute to your consideration of outbound investment screening.

At the outset, I will say that I believe we are engaged in one of history’s most consequential great power competitions, and that technology plays a key role in that contest. In the 1990s, I was as an officer on a Los Angeles class submarine. That boat was a tech marvel, carrying the world’s most sophisticated weapons and equipment, largely a result of America’s innovation ecosystem. My submarine service has made crystal clear the imperative for maintaining America’s technology advantage.

The PRC poses grave threats to the United States, its allies, and global order, including its strategy to exploit technology, raw materials, market power, and energy resources to achieve its ends. Key supply chains such as semiconductors are vulnerable to these same goals.

The 2018 enactment of FIRRMA and ECRA was largely in response to the potential risks arising from foreign actors’ activity with high-tech U.S. businesses. Now, both Congress and the Biden administration are considering a new agency with potentially sweeping powers to oversee American firms’ allocation of property and capital outside the United States.

A version of this interagency panel was considered in this year’s CHIPS bill. The regime would have limited investments, sharing of

Indo-Pacific, financing, and even sales that could benefit a country of concern, in a wide list of sectors. Key terms were broad and undefined and left substantial latitude to the Executive branch. Virtually every U.S. business transacting internationally could have been impacted. Subsequent proposals were narrowed, but I believe more homework is still necessary.

Recent reporting say that the Administration is close to creating establishing outbound screening by Executive order. I strongly believe that doing so would be a significant mistake. Rather, Congress is best suited to assess and respond to an issue of this complexity and potential scope and impact.

There should be no dispute that to ensure America's security the PRC's technology theft must be prevented. The question is whether a new and potentially far-reaching bureaucracy is the answer. The debate has taken on an apparent presumption that outbound screening is necessary, but decisionmakers would greatly benefit by resisting that temptation to rush into a "solution."

I commend the Committee for today's hearing. There should be more before any solution is enacted to define objectives and determine costs and benefits.

When a bipartisan Congress and the Trump administration collaborated to make the most extensive changes to CFIUS in its history, those efforts included roughly a half-dozen hearings with national security experts, the IC, the private sector, and former and current senior Administration officials. Congress and the President were thus well informed as to the gaps they intended to fill, the law's reach, and the attendant increases in capacity and cost. Afterwards, it took 2 intensive years within an existing CFIUS bureaucracy to effectively implement the law. Here, outbound screening would be out of whole cloth.

As with FIRREA, decisionmakers would be best served by building a comprehensive record, exploring whether existing or other authorities could be less bureaucratic and costly and more impactful. These options do not appear to have been fully considered, by they may, in fact, offer a better cost-benefit calculus.

My written testimony includes a foundational list of issues for a fulsome congressional examination of outbound screening.

From my CFIUS experience I know that a new screening mechanism would be time—and resource—intensive and require substantial effort to build a clear regulatory framework, and have the key human capital to ensure success.

It is an honor to contribute today to your scrutiny of this consequential matter. To H.L. Mencken is attributed the wisdom that "for every complicated problem there is a solution—easy, simple, and wrong." In the interests of national security, a strong, open economy, and accountable Government, all Americans should hope and expect policymakers to get this right. The alternative could be an unrestrained bureaucracy, wasted time and resources, and no meaningful response to the PRC's ominous goals. Thank you.

Chairman BROWN. Thank you, Mr. Feddo. This may be the only hearing ever where H.L. Mencken, and earlier Senator Cornyn quoted Lenin. The scope of that, I do not quite know how to analyze.

Mr. Strayer, you are recognized for 5 minutes. Thank you.

STATEMENT OF ROBERT STRAYER, EXECUTIVE VICE PRESIDENT OF POLICY, INFORMATION TECHNOLOGY INDUSTRY COUNCIL

Mr. STRAYER. Mr. Chairman, Ranking Member Toomey, I am currently the lead of the global policy team at the Information Technology Industry Council, or ITI. ITI represents 80 global leading companies from across the ICT sector, including hardware, software, semiconductors, network equipment and cybersecurity.

The U.S. Government has no more important responsibility than to protect the Nation's security. ITI therefore commends the Committee for holding this hearing. It is essential that there be a structured, deliberative process to include the views of all stakeholders on outbound investments. We also appreciate the leadership of Senators Cornyn and Casey on this issue and for their letter this week calling for robust stakeholder engagement.

We are committed to working with Congress and the Administration to achieve effective national security outcomes. U.S. national security depends on continued U.S. technological leadership. Today, other Nations and their companies are competing to find the next transformational technology.

Global competition in tech innovation is occurring in increasingly rapid cycles. U.S. companies must use the profits earned from global sales of current products to fund future R&D of the next improved generation of products. Companies also face fierce competition on cost and efficiency. U.S. companies use global supply chains to access the best talent, components, and manufacturing capabilities to be competitive. Global markets for sales and diversified supply chains are therefore vital to American technological leadership, and that leadership contributes to a shared goal of enhancing U.S. national security.

U.S. Government policies have helped companies run faster and better compete in global markets. The incentives in the recently enacted CHIPS and Science Act are a good example of incentives to buildup U.S. tech capabilities. ITI was a steadfast supporter of this legislation and appreciate Congress passing that legislation.

As U.S. Government examines ways to maintain its technological advantage and protect national security, there are five considerations that will help an outbound investment framework be successful.

First, it is imperative that policymakers examine existing authorities, identify gaps that implicate national security, and craft new authorities in a manner that is sufficiently narrow to avoid capturing transactions already subject to existing regimes. For example, U.S. Commerce Department has extensive authority to restrict the transfer of technology, software, and commodities to and from countries and entities of concern.

Second, we should be specific and targeted about national security risks of the technologies and investments to be covered. My perspective on this point is shaped by my time at the U.S. State Department. I served as the Deputy Assistant Secretary for Cyber Policy there. In that role, I was responsible for leading the U.S. Government's international 5G security campaign, and I was also involved in planning to protect U.S. technology networks.

In 2018, we identified that significant risk was related to one particular type of technology platform, wireless 5G networks, and we focused the U.S. Government on a governmentwide campaign to establish policies to protect the United States and convince our foreign partners and allies to adopt consistent policies that were based on a governmentwide strategy.

A similar degree of focus on particular technologies is needed for the U.S. Government to be successful in outbound investment screening. Its scope needs to be manageable and enforceable, and the rationale must be understood by the private sector and allied Governments. An assessment of emerging technologies should be done by the intelligence community and other experts in U.S. Government and in the private sector. That would help identify the most transformative technologies and consider their impacts on economic growth, national security, and military capabilities, as well as an adversary's ability to monopolize that technology. That analysis should take place before a framework enters into force.

Third, U.S. Government should consult with industry regularly. The private sector has the best data and understanding of supply chains. It can share this information with the Government to design policies that achieve U.S. goals while minimizing costs to supply chains.

Fourth, companies need as much certainty as possible to plan and time to adjust their supply chains. In most cases, those take years to develop. The best way to provide certainty is with clear lines about the investments that would be covered by regulatory restrictions.

Fifth, build international coalitions. It is critically important that new regulatory mechanisms be coordinated with U.S. allies and partners to ensure that U.S. actions do not cause investments to leave the United States and be made through countries that do not have similar investment restrictions.

Thank you for the opportunity to testify today, and I look forward to your questions.

Chairman BROWN. Thank you, Mr. Strayer. Thank you all for your thoughtful comments on a complicated subject.

I will start with you Dr. Bauerle Danzman, if I could. You state that there are, quote, "gaps," unquote, in the U.S.'s ability to address national security risks associated with outbound investment. Elaborate if you would on what those gaps are and the type of risks associated with those gaps.

Ms. BAUERLE DANZMAN. Absolutely. So, you know, when we are talking about gaps in authority we are really addressing whether there are certain kinds of intangible benefits that U.S. investment provides that are separate from technology transfer and thereby not addressable through export controls.

I lay out some of this in my written testimony, but I really focus on two kinds of active investments, FDI and venture capital. Let us set aside portfolio flows which are just passive financial investments and not suitable for screening.

For FDI, for example, a semiconductor company building a fabrication plant in China or a software development company opening an AI R&D facility in China, there is a vast literature on the role of FDI in broader economic development of receiving States.

This literature focuses on identifying positive spillovers to local industry from FDI, usually through knowledge, knowhow, and market-making channels. Multinationals can act as catalysts for domestic industry. They do so even through these non-tech transfer channels. Multinationals help foster indigenous industries by incorporating local firms into their supply chains, by importing knowledge about international markets, through building connections to multinationals' broader supplier and buyer networks, and by transferring managerial practices that encourage efficiency and quality control.

We know that by interacting with multinationals, domestic firms gain foreign market knowledge to directly compete in international markets, and domestic firms that integrate into multinational supply chains are actually statistically significantly more likely to become exporters, to increase their ability to supply the domestic market, as well as to produce higher quality and more complex products. This is how developing countries move up the value chain.

And these are all less tangible contributions to the domestic market that are not controllable through export controls, and normally they should not be. Normally all of these spillover effects of FDI are beneficial to economic development, and this is a success story that illustrates how economic integration can generate shared prosperity.

So in general, this is a good thing for everyone involved. But in very narrow cases, we may want to prevent U.S. firms from building China's innovation ecosystem in technologies that are so vital to U.S. national security that we just cannot afford to cede that tech to the PRC.

And then in terms of venture capital, we all know that the whole point of venture capital is not to just the investment but that investors provide mentorship and advice to founders who need substantial strategic and logistical help to scale up their businesses. Venture capital play prominent roles on corporation boards. They provide founders and their teams with access to investors' financial, commercial, professional, and even political networks. A company with VC funding is able to leverage the legitimacy of its funder to find more investors, board members, and customers.

Again, venture is an essential part of our innovation ecosystem. Forty-two percent of U.S. companies that went public from 1974 to 2015 were venture-backed. So as a general matter we should encourage venture. But on the flip side, these same features that have been so central to the journey from startup to commercial viability in the United States could generate national security risks if U.S. venture contributes to critical technology startups in countries of concern.

Chairman BROWN. Thank you. Let me ask you another question, and we are down to about a minute.

Ms. BAUERLE DANZMAN. Sorry.

Chairman BROWN. In the paper you coauthored with Emily Kilcrease you call for a broad notification requirement that would provide additional information to investors dealing with certain investments. How should policymakers consider the scope of such a notification requirement?

Ms. BAUERLE DANZMAN. So in that paper we believe that starting with export controls is a kind of good way to mirror. Basically, outbound review should mirror U.S. export controls, similar to the solution that Senator Toomey afforded just a few minutes ago. So if you need a license to export an item to China you would need a review before investing in a Chinese company developing or operating in that same technology.

The inevitable criticism of that approach is that it leaves out emerging technologies. So we also suggest that it may be useful to go through a process of narrowing the critical and emerging technology list to a few areas that matter on that list as well that are not currently controlled. The important part there is to have a public notice and comment period that really allows to get down to greater specificity in terms of what the precise technology would be so that it is administrable.

Chairman BROWN. Thank you. Senator Toomey.

Senator TOOMEY. Thank you, Mr. Chairman. You know, I quoted Jake Sullivan's definition or indication of why this was necessary, in which he said the problem is "circumvent the spirit of export controls," I do not quote that because I want to criticize or mock this. What I want to do is underscore the sort of imprecise and vague and not terribly well-defined nature of the problem we are trying to solve.

So maybe we could, and Professor, I have to ask you to be very, very short if you could, if you could give us a specific example of a transaction, a process, something that is not captured under existing export controls, and you think we would all agree is problematic.

Ms. BAUERLE DANZMAN. Sure. So I do not claim to speak for the National Security Advisor, and I also share many of the concerns that you mentioned before about making sure to scope.

Senator TOOMEY. Right.

Ms. BAUERLE DANZMAN. But as a hypothetical, you know, Commerce recently announced four new tech controls under Section 1758. One newly controlled technology is a specific electronic computer aid design software.

Senator TOOMEY. OK, but this is—just to be clear, this is a hypothetical.

Ms. BAUERLE DANZMAN. Right. This is a hypothetical. I do not want to talk about specific transactions.

Senator TOOMEY. Do you know of specific transactions?

Ms. BAUERLE DANZMAN. Yes, but I do not want to talk about specific transactions that would implicate particular companies. So I am just saying that if a U.S. company invested in a Chinese entity that was trying to develop this controlled technology indigenously, but it was trying to develop it indigenously without using U.S.-controlled tech, that would be an indication, in my mind, of a company trying to circumvent the spirit of export controls.

Senator TOOMEY. All right. There is another aspect to this. Maybe Mr. Ashooh—am I saying that correctly?

Mr. ASHOOH. It rhymes with cashew.

Senator TOOMEY. OK. China has obviously got a lot of accumulated capital. Plenty of money. Government has enormous resources. Private sector has enormous resources. So would you agree

that if there is a problem here, the problem is not providing money. The problem is something else. And we know that the export restriction regime has the ability to limit the export of products, including software.

So it seems to me what we are really getting at here, what comes up periodically in the discussion, is this much more difficult to define concept of like knowhow, expertise, professionalism, process, a way of doing business that is likely to enhance your ability to be successful. How would you react to that characterization of what seems to me to be the thing that folks are going after?

Mr. ASHOOH. Thank you for the question, Senator. I actually think there is only one area that, in a specific way, presents a disconnect between the goals and the authorities, and that is cash money. It is conceivable that an end user that would be export restricted could still receive U.S. investment, and that to me is a disconnect. I do not have a specific example because during my time at BIS I did not encounter one.

But I think it is important to, on the question of associated transfer of intangibles, like knowhow, the Export Administration Regulations covers that. It defines technology primarily as information. So it is important to think, it is not just the phone or this pen, it is the manual that goes with it. That is technology. That is controlled, in whatever form, usually intangible, that it goes.

So we have a very robust and textured series of regulations that are already in place that with some adjustment could address whatever concerns there are.

Senator TOOMEY. Mr. Feddo, I wonder if you could address, we are at a situation where we might have an Executive order come out in the absence of legislation. We might be able to get legislation done. Could you just discuss a little bit your sense of how important it is that whatever is done here is defined in statute by Congress?

Mr. FEDDO. Senator, I think this is the prerogative of the Congress. It is Article I of the Constitution for a reason, and you have explicit authority to regulate commerce with foreign Nations. Such a complicated issue and question, and the problem has not been sufficiently designed. An Executive order that creates this committee, when you create a committee like this, a bureaucracy, it is not going to be unrung.

But there are so many questions, as I list in my written testimony, that I think need to be answered, in terms of capacity—how many transactions we expect to capture, what sort of risk analysis would be involved, how are we going to fund this committee, accountability, who is in charge, and has the institutional heft within the Executive branch to move forward and implement it in an appropriate way, and then answer to committees of jurisdiction in oversight? All of that comes with legislation and not necessarily with an Executive order.

A statute also gives an opportunity, as I have maintained, for the Congress to build a record, to get folks from the Administration on the record to identify the problem and answer precisely the question you just posed to my fellow witnesses about an example of a gap. Those sorts of thing we did during FIRRMA. Treasury Department, Commerce, DoD came up here and worked with you all and

explained gaps. We had the intelligence community brief the Congress on the gaps that needed to be filled.

As far as I am aware, that sort of dialogue and establishment of a record and a foundation for this kind of committee has not yet been executed here.

Senator TOOMEY. Thank you very much. Thank you, Mr. Chairman.

Chairman BROWN. Thank you, Senator Toomey.

Senator Menendez, of New Jersey, is recognized.

Senator MENENDEZ. Thank you, Mr. Chairman.

As a country we need to consider, I believe, how we regulate outbound investments of critical sectors as part of our broader economic resiliency strategy. The COVID pandemic revealed structural weaknesses in the United States supply chain, and we are still feeling the pain of those vulnerabilities today.

So Professor Danzman, what were some of the consequences of having so much of our critical production abroad, particularly in countries like China?

Ms. BAUERLE DANZMAN. Thank you for the question. I think that when we think specifically about the supply chain shocks that we experienced because of COVID we should separate out what were demand shocks plus supply shocks of zero COVID policy versus national security concerns for extended periods of time. So the CHIPS Act, in particular, has been working to—you know, the idea behind that is to bring back some supply and to diversify the supply chain so that we are not over-reliant on just a few nodes in the chip supply chain.

But I think that we want to be careful to not overlearn the example of the COVID pandemic, which was very much about shocks to the system that are now working themselves out.

Senator MENENDEZ. Yeah. But it is interesting, shocks to the system that we are working out. But at the same time we had doctors and nurses who had to improvise in the creation of personal protective gear as we struggled to get it from other parts of the world. I do not know what the next virus will be. There will be one at some point, and hopefully not, but at some point there will be one, and we have to think about that.

Let me ask you, would lack of a comprehensive outbound investment strategy for certain critical sectors mitigate the benefits of recent efforts to strengthen our supply chains?

Ms. BAUERLE DANZMAN. Well, I think when we consider the reasons why firms move overseas it is normally because of commercial viability in the U.S. And so if the goal of the Congress is to ensure that we retain some amount of domestic capabilities, there are other measures that we should use beyond prohibiting outbound investment to actually help on the side of making those types of investments in the U.S. commercially viable.

Senator MENENDEZ. OK. Well, I believe our lack of outbound investment oversight in the sensitive industries has the potential to hamper the competitiveness of our firms. Practices such as intellectual property theft are all too common in parts of the world, especially China, which harm the ability of U.S. firms that are playing by the rules to compete.

Mr. Feddo and Mr. Ashooh, how has the stolen intellectual property in countries like China degraded our economic competitiveness and national security?

Mr. ASHOOH. Thank you for the question, Senator. It is an incredibly important issue. It is hard to measure how it has degraded because, regrettably, it is not limited only to China. Intellectual property theft is a global issue, quite frankly, which makes it all the harder to deal with.

And during my time at BIS we were often confronted with the question that in the presence of an IP violation should we then take an export action? And that was a reasonable request because the ability to deal with IP theft in the courts is insufficient. The bomb has already gone off. The information has already been purloined, and even if you pursue legal action, how do you undo that? You cannot really disgorge the IP.

Export controls as a solution to that are not ideal. So it is worth us contemplating how else to get at it, because the legal system, it is important, it is necessary, it needs to be used, but it does not necessarily solve the problem.

Mr. FEDDO. Sir, thank you for the question. I will just add, recently FBI director Wray commented that every 12 hours the FBI is opening a new investigation related to espionage or hacking or something that relates to theft of intellectual property.

The FBI actually has on its website a wheel of doom, I will call it, that lists all of the different ways that the CCP steals our technology, everything from espionage to hacking to research partnership to academic institutions, inbound investment, the CFIUS problem. And so all of that is part of the calculus, and his estimate was, his comment was that over 2,000 active investigations by the FBI at the time he made the comment.

And so I am not sure how to quantify that, but I think that the damage to our intellectual property and our knowhow is profound. What I would say is to me it brings home the point that we need more information. I think many who have testified today have commented. We do not fully understand the problem, and so we need to gather more data, the problem that is with risk from outbound investment and how it compares, for example, to hacking and espionage and the other risks that we face and whether the cost-benefit is there with respect to how much resources we dedicate to one versus another.

Senator MENENDEZ. Yeah. I would just close by saying I think that maybe one of the things that outbound investment would help us with, it seems to me that we want American companies, obviously, to continue to compete in the global economy. By the same token, it seems to me that we need to preserve the apex, the tip of the iceberg, of the most sophisticated, sensitive elements that we need to preserve to have a competitive edge and a security edge. And that the rest of what is underneath of that tip, that might be generally commercially available, is a way to look at how we can continue to be competitive.

But I think there are some sectors, it seems to me, that we have to be concerned about, not only the economic equation but the security equation as well.

Thank you very much.

Chairman BROWN. Senator Tester, of Montana, is recognized.

Senator TESTER. Thank you, Mr. Chairman, and I want to thank the folks that are here testifying today. I appreciate your testimony.

In my real life I am a farmer, and I have been on the land, between my parents, grandparents, myself, for 110 years-plus. One of the things that I am somewhat concerned about, which is why I am asking the question, is the potential to buy up farmland from a foreign country, potentially even a foreign adversary country.

I will direct to you, Mr. Feddo, but anybody can jump in if you want to add value, and that his, is this something that we are seeing, number one, or is this something that we are even tracking?

Mr. FEDDO. I will answer the second part first. I am not sure to what extent we are tracking it. I have seen, as to whether it is a problem, I am aware that there is increasing reporting about buying up land. Certainly with respect to CFIUS, the Congress provided the Committee jurisdiction over real estate investments, land investments close to military installations and otherwise. That provides us some overlap, some jurisdiction to look at those types of investments. But as to other agriculture-related investments I am not aware of the scope of the problem. But it is something that attention has been raised, and I think is worth this Committee and others thinking about.

Senator TESTER. Anybody else want to add to that?

[No response.]

Senator TESTER. So I appreciate your answer and I understand we cannot look at everything. But the fact that we are not doing this, and food supply is pretty critical to national security—and you can screw the food supply up pretty easily. The thought comes to my mind about putting nitrogen fertilizer in grain, which adds protein on a test but also poisons the product, is a big deal.

I mean, whose job would it be to look at that? I am talking about people buying land up in the U.S. Do we have an agency that would?

Mr. ASHOOH. I think it was appropriate to direct the question to Tom because I think CFIUS does exist to look at national security, implications of acquisitions. And the real estate scope did grow substantially. I think, Senator, what you are saying in this is a very good thought, which is food security is really an infrastructure issue, which has grown to become a national security issue. So my view is the authority is there. Getting those definitions right is something that with Congress' help should be looked at.

Senator TESTER. How about from an agribusiness standpoint? Do we look at that at all, do you know? I will say to you, Mr. Feddo, again, how about foreign purchasing of agribusinesses? Is anybody looking at that?

Mr. ASHOOH. Absolutely. I mean, that is the core jurisdiction of the committee. If a foreign business buys a U.S. business it is within the jurisdiction for consideration of national security risk.

Senator TESTER. So I probably need to visit with some of you offline, but I will just give you an example. And I am not saying that these guys are not legit. I do not know that they are. I do not know that they are not. But there is a lot of land being purchased around me, in north-central Montana, by Canadians. I do not know if it is

Canadian money, though. It may be money from somewhere else. And if nobody is checking this out—and I do not know how hard it would be to check this out. I just do not know—it seems to me that we are opening ourselves up for a risk that we might regret later. That is all.

So the previous question. Senator Menendez was talking about intellectual property theft and research partners and universities is one of the places. I will go to you, Ms. Danzman, because you are from Indiana University, a great university in this country. Is the university aware that there might be—look, we have a very open Government and we wanted to work together and share information. I think it is foundational to who we are as a Nation, by the way. But when people are trying to steal stuff, that puts a little different light on it.

Is a place like Indiana University aware of what kind of threats are out there when we are talking particularly about research but it could fall into a lot of other areas too.

Ms. BAUERLE DANZMAN. I appreciate the question. You know, academics really value the openness of science, and so that is an important part of what it means to be in the global academy. At the same time, it is the case—I know that the FBI goes around to universities and works with universities to discuss the risks that we currently need to be thinking about in our current environment, particularly around the development of technologies that do have important dual use. And I think that is a very important thing for the FBI to be doing, and that program should be probably expanded.

Senator TESTER. OK. So you think it is important what they are doing but the adequacy may need to be—the adequacy is not where it needs to be?

Ms. BAUERLE DANZMAN. You might also look at in the EU there has been some recent movement on this issue, specifically around who is funding universities and university research. So this is an issue that I imagine the U.S. and EU Trade and Technology Council is also engaged with as well.

Senator TESTER. The more I learn, the more I am scared. Thanks.

Chairman BROWN. Thank you, Senator Tester.

Senator Warren, from Massachusetts, is recognized.

Senator WARREN. Thank you, Mr. Chairman.

So last month President Biden made a historic investment in our future by signing the CHIPS and Science Act into law. In addition to boosting Federal funding for scientific research—yay—the law provides \$52 billion in subsidies to revitalize our domestic semiconductor manufacturing industry.

Semiconductor chips are critical ingredients for everything from cellphones to cars, so this is a very important investment to strengthen our supply chains, create good union jobs, and bring down prices for consumers.

But to ensure that corporations exclusively use CHIPS funds for these purposes rather than simply for boosting their own profits, Congress put guardrails up, and one of these guardrails prohibits semiconductor manufacturers from using CHIPS funds for buying back their own stock. Stock buybacks mainly serve to manipulate

share prices and boost corporate executives' profits, money that could instead be used to build a factor or hire workers or invest in worker training.

So Dr. Bauerle Danzman, you are an expert on investment in critical sectors like semiconductors, so let me just ask you. The CHIPS and Science Act clearly prohibits chip manufacturers, like Intel or IBM, from using CHIPS funds to conduct stock buybacks. But could Intel or IBM accept CHIPS funds and then use its own money for stock buybacks?

Ms. BAUERLE DANZMAN. Possibly.

Senator WARREN. All right. So here is the issue. If Intel is awarded CHIPS funds it is required to use those funds to fulfill the purposes of the CHIPS program. I totally get this. But money is money. Money is fungible. By taking CHIPS funds, Intel would have more money, which might free up other funds that it could then use for stock buybacks.

You know, this is not a hypothetical risk. Between 2011 and 2020, five of the largest semiconductor companies—Intel, IBM, Qualcomm, Texas Instruments, and Broadcom—all of which heavily lobbied for the CHIPS Act, spent \$250 billion, or 70 percent of their collective profits, five times more than we put into the CHIPS Act, on what? On stock buybacks. Just a few weeks ago, Texas Instruments authorized a new, \$15 billion stock buyback program.

Now Secretary Raimondo says CHIPS funds will not be used for buybacks on her watch, period. Commerce said CHIPS money is not, quote, “a subsidy for companies to make them more profitable or enable them to have more cash for stock buybacks or to pad their bottom lines,” end quote.

So, Dr. Bauerle Danzman, why is it important that the Commerce Department lives up to its promises that taxpayer funds in the CHIPS programs are not used, directly or indirectly, to fund stock buybacks or other shareholder payouts?

Ms. BAUERLE DANZMAN. Thank you for the question. It is important. You know, when you are designing these sorts of subsidy programs it is important to get the balance right because you want the companies to actually take the funds and to expand production, which is good for national security and good for American workers.

That said, taxpayers are investing billions of dollars in the semiconductor manufacturing industry on the basis of two things, right, the U.S. will be physically safer and more economically resilient if we build back more of this capacity, and that reshoring is not commercially viable without Government support.

And so if we see a lot of stock buybacks this is going to undermine the U.S. public support for these sorts of programs, and that will make it harder to appropriate such funds in the future, as well if we are not expanding domestic production as much as we should, that could have national security consequences.

Senator WARREN. Thank you very much. You got a lot of points in there about why it is important that the money we invest means that the companies are spending money on reinvesting and not on something like stock buybacks.

How do we get there? That means tougher rules like requiring companies on the application to attest that they will not engage in stock buybacks, by giving additional preferences to companies that

commit to longer buyback moratoria, by clawing back funds from companies that go back on their word.

So I am looking forward to working with Secretary Raimondo and my colleagues to ensure that this critical investment onshores our supply chain, creates those good union jobs, lowers prices for families, and powers our economy into the future in ways we intended, rather than helps line the pockets of the CEOs of these giant corporation.

I appreciate your work in this area, and I hope we can work together to get this done. Thank you.

Chairman BROWN. Thank you, Senator Warren.

Senator Van Hollen, of Maryland, is recognized.

Senator VAN HOLLEN. Thank you, Mr. Chairman, and thank you for having this hearing. I thank all of you for your testimony. I think we can all agree that it is important for the United States to maintain its competitive edge in areas that are critical to our national security, our economy, areas of strategic importance.

The CHIPS and Science Bill, which we passed, was a really important part of that. Making sure that we do our business here at home is a critical piece. Another piece is to make sure we do not allow companies and a lot of companies associated with foreign Governments to steal U.S. intellectual property.

Senator Sasse and I introduced a bill that is part of the current conference of what remains of USICA, to do that so that U.S. companies who have had their IP stolen do not have to take a case-at-a-time approach on patent infringement, but the U.S. Government can take action through sanctions to make it very clear that we are not going to be firing with an economic BB gun but we are going to have more strength.

The third is this topic that we are discussing today, and I do think most of us share a concern that without some sufficient Government oversight, transparency, guidelines, that U.S. outbound investment could strengthen the capabilities of China or other adversaries in areas that are of strategic importance to the United States. I mean, that is what we are focused on here.

I think there are good-faith disagreements as to how you define the scope, exactly what the mechanism is to implement that. But it does seem to me that in order to be effective, in addition to figuring out how we want to do this here at home, what kind of mechanism we want, we also have to make sure that our allied partners adopt similar mechanisms.

Ms. Danzman, would you agree with that?

Ms. BAUERLE DANZMAN. I do not think you can overstate the importance of multilateral engagement on this issue.

Senator VAN HOLLEN. Right. And just each of you, yes or no, in terms of whether you agree with that principle.

Mr. ASHOOH. I strongly agree.

Mr. FEDDO. Likewise. Multilateral efforts area always stronger than going in alone.

Mr. STRAYER. Agree.

Senator VAN HOLLEN. Right. So, you know, with FIRMA we created a mechanism to create incentive for our partners overseas, allies overseas, to adopt similar mechanisms to our CFIUS process. And it seems to me whatever we decide in terms of the shape and

form of rules that apply to outbound investment or transparency, it will only be effective if we get our partners around the world to adopt it, for a couple of reasons. One is if they do not, they can send capital to support the same sort of investments in strategically important areas, and number two, that would then put U.S. firms at a disadvantage because we are essentially saying that we are not going to allow this but leave the door open for others.

Can you address where we stand right now in those conversations, and are there any of our partner countries today who have adopted a screening process on their outbound investment? I do not know who would be best to answer that.

Mr. ASHOOH. I can at least make an initial comment. I am aware that outbound screening exists in some of our allied partners, but I would like to take a moment to talk about the multilateralism that exists today. There is a bit of a common theme here among the witnesses, which is that an initial step in any outbound screening criteria should be to synchronize it with the existing national security criteria that exists between CFIUS and the Export Control System, and to look at whether or not outbound screening should align with that.

Export controls are overwhelmingly multilateral, so that work is already in place in many ways—not completely. Work needs to be done. But there is a lot to work with there right now.

Senator VAN HOLLEN. Any others? Ms. Danzman?

Ms. BAUERLE DANZMAN. Sure. So both South Korea and Taiwan have very narrowly scoped outbound screening mechanisms so that answers one of your questions. I am not currently in the Government so I do not know how much there has been discussion at the multilateral level specifically around this issue, but in informal conversations with those over in the EU, this seems like this is going to really take a long time to develop a shared understanding of the problem and of the likely best solutions to such a problem.

Senator VAN HOLLEN. I appreciate that. You know, I was overseas a number of years ago, before the COVID outbreak, and there was a lot of discussion on the CFIUS rules and getting the EU and other partners to align some of their rules with that. And I think we are going to have to go through the same kind of process with respect to this regime, you know, once we get a better sense of what we want to do and what those rules should be. I appreciate all of your agreement that that is an essential piece of any successful mechanism. Thank you.

Chairman BROWN. Thank you, Senator Van Hollen.

Senator Warner, from Virginia, is recognized from his office.

Senator WARNER. Thank you, Mr. Chairman, and thank you for having this hearing. I think it is critically important, and getting this right is a challenge.

I am going to talk for a minute or two before I ask questions about the fact that this has been such a focus of the Intelligence Committee over the last 4 years. As a matter of fact, there was always a disconnect between what I was hearing from business circles and what I was hearing from the intelligence community about the enormous challenges and threats posed by the PRC. And let me be clear that my beef is with the Communist Party of China and

Xi Jinping's leadership. It is not with the Chinese people or the Chinese diaspora here in America or anywhere else in the world.

But we have to acknowledge that there is no such thing as an independent company in China at this point. Chinese law dictates that all these companies have to be first and foremost loyal to the Communist Party, not their shareholders. So starting in 2018, we have now had 21 separate classified road-show briefings to alert industry sector by industry sector of this challenge.

I think we have made progress, and I think even groups like private equity, which were reluctant to hear this story at first because they were making so much money in Chinese tech companies, are starting to get the message, the level of intellectual property theft, the level of China investing not just directly but through subsidiaries. I am going to come back to that in a moment with my question.

But this technology competition, I think, is the challenge of our time. We have got to deal with Russia, obviously, and Ukraine, but the technology competition with the PRC going forward, we have never faced this kind of economic competitor.

And I would say to my colleagues, you know, and I know we have to get the CHIPS bill right, but without the CHIPS bill there would not be another chip manufacturing plant built in America. You know, you look at the last 15, 18 years, I think there has been over 120 chip fabs built around the world. Only 17 of them built in America. And every country around the world has this kind of program. We can either complain about that or we can get in the game in terms of competition. And I think what we are doing in chips we are going to have to do in other technology domains in a very, very careful way.

But I want to start my question with Dr. Danzman, and one of the things that you have talked about in your statement was the idea of we need to think about this issue in almost network terms, because what we have seen, particularly in terms of our challenges with China, not only intellectual property theft, not only kind of Chinese inbound investments in the form of venture firms and other entities, but increasing we are seeing China mask these activities through investments in, for example, European subsidiaries. And you have talked about some of the leakage that takes place, and my fear is that while there are some new entities out there trying to clearly identify the supply chain, because I have seen private enterprises that indicate you go second or third level suppliers, and even now we have got firms that are reliant upon China and Russia sources.

Do we know enough about kind of the overall supply chain so that whether it is inbound investing or outbound investing we have a good idea of identifying who we ought to be monitoring and making sure that we are accurately assessing the threats on investments?

Ms. BAUERLE DANZMAN. Thank you very much for the question. I am happy to talk longer afterwards because this could be a long question and I want to keep my answer short.

There are kind of two aspects that I think are important here in your question. One is about entity resolution, which is how do we know who actually owns or who controls the entity that is invest-

ing. I think that we do have good intelligence and good ability, in the U.S., at least, to track that entity resolution quite well, but sometimes that is not something that all of our partners and allies have access to.

But on kind of the broader question of how do we know what is going on in the supply chain, one thing that we have learned is that not even companies oftentimes know what is happening throughout their supply chain. Normally there is knowledge first-tier suppliers, but going down into the second and third tiers, so the suppliers to the suppliers, and the suppliers to the suppliers to the suppliers, there is not a lot of understanding of how that whole system works.

Senator WARNER. Yeah, and I think there, and let me just quickly say, I want to make one last point. I am not going to get another question in. But there are private sector entities. There is a company in Virginia called Interos that tracks some of this. I think we need to have more of those sources.

I do not have time for a question but I will point out, Mr. Chairman, that we ought to not only look at outbound investment but I do think we need to call into question, for example, Apple is a great American company. The idea that they are potentially buying lots of their semiconductor chips from YMTC frankly strengthens China's position in that market, and it is something that I know Senator Rubio and I and the Intel Committee have raised questions. And I think we need to look at this issue as well.

Thank you very much, Mr. Chairman.

Chairman BROWN. Thank you, Senator Warner.

Senator Toomey and I would like to do a second round. It will take no more than 10 minutes, probably less, and we are also called to a vote at 11:30.

I have a question together for Mr. Feddo and Mr. Ashooh. You both have experience working in positions that review the national security risks associated with certain business transactions. I will start, Mr. Ashooh, with you. Based on your Government experience, if policymakers established a notification requirement what information would be helpful to collect?

Mr. ASHOOH. Well, the most important information would be whether or not whatever they are engaged in intersects with our export restrictions. That currently exists right now, under CFIUS, thanks to FIRRMA. Mandatory declarations are required, where there is critical technology that requires a license involved. I think, again, building on what works, that is a place I would start.

Chairman BROWN. And Mr. Feddo, same question. What information would be helpful to collection, in your mind?

Mr. FEDDO. I agree with Mr. Ashooh. I also think this is a place where relying on the IC and the FBI to identify certain sectors of greatest risk with respect to this outbound investment question and have that inform where we are asking for reporting, because in some cases there may not be export controls but it is a cutting-edge technology that we need to know more about.

Chairman BROWN. Thank you, Mr. Feddo. Senator Toomey.

Senator TOOMEY. Thanks, Mr. Chairman. So, you know, I remain concerned about how well-defined the problem we are trying to address actually is. I think I have heard that maybe the gap between

what we are able to limit now and what we might wish to might just be cash. I think we have heard a discussion about how there are these processes and knowhow, which seems extremely difficult to define.

Let me ask this, and I think I would just put this to each of our panelists. If we do go down the road of standing up an outbound screening notification regime, how important do you think it is that we limit the application to very precise and well-defined boundaries and maybe even the importance that these boundaries be a reference to existing law that recognizes, that has already identified technologies that we are concerned about? We have got very limit time—I apologize for that—but maybe we could start with Mr. Strayer and work our way down.

Mr. STRAYER. Yes, Senator. I very much agree that we need to be very precise about how we are identifying those technologies. But the other thing that I have heard multiple times suggested is just because something is on the Commerce Control List that should immediately be something that is sought to be controlled in the investment level. But one needs to understand that the Commerce Department's Export Control List is very specific. So if there is an AI technology in a specific application added somewhere to the Commerce Control List, that should not prohibit investment in all artificial intelligence.

So that translation is going to be very hard. It needs to be precise for the reasons I outlined in my technology.

Senator TOOMEY. Thank you. Mr. Feddo?

Mr. FEDDO. I agree, precision is imperative if we move forward with this, compliance costs for the private sector. Even entities that are not necessarily directly impacted by this will have compliance costs and will need to consult with advisors and lawyers and others to make sure that they are on the right side of the law. So specificity is imperative.

Senator TOOMEY. Thank you.

Mr. ASHOH. Yeah, I fully agree. In fact, I would say the power of our existing Export Control System, and it is powerful, is in its specificity because it allows commerce to flow freely where we are not doing the restricting.

Senator TOOMEY. Thank you. Professor?

Ms. BAUERLE DANZMAN. I will just agree. I think it is really important to have clarify for the certainty it will provide to firms about what it is that they need to be worried about when they are thinking about outbound investment. Thank you, Mr. Chairman.

Chairman BROWN. Thank you, Senator Toomey.

Thanks to the witnesses. Thanks to the four of you today for your thoughtful, helpful testimony.

Senators wishing to submit questions for the record, they are due 1 week from today, Thursday, October 6th, and we ask you, as witnesses, to please submit the responses to those questions for the record within 45 days from the day you receive them.

Thank you again for joining us. The Committee is adjourned. Thank you.

[Whereupon, at 11:37 a.m., the hearing was adjourned.]

[Prepared statements, responses to written questions, and additional material supplied for the record follow:]

PREPARED STATEMENT OF CHAIRMAN SHERROD BROWN

Earlier this year Secretary of State Antony Blinken said that, “Beijing wants to put itself at the center of global innovation and manufacturing, increase other countries’ technological dependence, and then use that dependence to impose its foreign policy preference.”

“And Beijing is going to great lengths to win this contest.”

It is critical that the Administration has the tools it needs to protect our national security.

And this Committee has played a key role. We’ve done that through export controls that restrict the flow of sensitive technology.

And we’ve done that through the screening of foreign direct investment into the U.S., to guard against adversaries accessing our technology or critical infrastructure capabilities.

Four years ago, we enacted the Export Control Reform Act, known as ECRA, which provided permanent statutory authority for the U.S. Government to regulate U.S. exports that have commercial and defense applications.

Those controls can apply to important technology, like semiconductors. They can apply to the way a technology is used, like military intelligence. And they can apply to who uses it, like a Chinese quantum computing company.

Along with ECRA, we also passed the Foreign Investment Risk Review Modernization Act, known as FIRRMA.

That law strengthened and expanded the jurisdiction of the Committee on Foreign Investment in the United States, known as CFIUS, that reviews foreign investments, like mergers or acquisitions, of U.S. businesses.

We passed these bipartisan laws, because we all recognize the importance of maintaining U.S. technological leadership, and the need to protect that leadership.

We know that threats to our national security are evolving. We also know that our adversaries will use any means they can to close the gaps between our technological capabilities and theirs—without much care to how legal their tactics are.

What we don’t know is to what degree U.S. investments are helping them close those gaps.

U.S. investments—whether from a venture capitalist or pension fund—could wittingly or unwittingly support foreign technological investments that, in the words of our Secretary of State, could “increase other countries’ technological dependence, and then use that dependence to impose its foreign policy preference.”

We cannot let that happen.

It’s why policymakers have been examining the role that U.S. investments abroad are playing to enable foreign adversaries, as they develop technologies that could take away our technological edge and damage our national security.

Senators Casey and Cornyn introduced a bill designed to address these concerns by requiring notifications of certain investments, and enabling the President to prohibit others.

Without objection, I’d like to enter into the record letters of support for that bill—the first from Representatives Rosa DeLauro and Bill Pascrell, who introduced companion legislation in the House, and the second from the AFL–CIO, which supports that legislation.

We need to better understand whether U.S. investments abroad pose national security risks to the United States. In a global economy where capital flows freely, we need to ensure that we are not investing in technologies that harm our national security.

Prior to creating CFIUS, we had not systematically tracked foreign investments into the United States.

Times change, and so do the threats we face.

We must understand the scope of outbound investment and address the impact it plays in supporting efforts by our adversaries to achieve their “foreign policy preferences.”

Protecting U.S. technological leadership is an important part of this conversation, and it’s why we’re here today.

It’s also not the whole story.

Part of this story is an issue that Ohioans know all too well.

Over the last 30, 40 years, corporations searched the globe for cheap labor. First, they went to anti-union States in the South.

Then, corporations lobbied for tax breaks and bad trade deals to help move jobs overseas—always in search of lower wages.

They started with manufacturing jobs, but they didn’t stop there—corporations moved R&D jobs abroad too.

And Wall Street rewarded them for it, over and over and over.

In some cases, investments abroad outpaced investments in American workers. It undermined our national security and hollowed out our middle class.

Protecting technological leadership and protecting jobs are connected. Ohioans know how much innovation happens on the shop floor.

Investing in our workers, our infrastructure, our educational system, and our research, development, and manufacturing ecosystem will help shore up supply chains.

From the Infrastructure bill to the CHIPS and Science Act to the Inflation Reduction Act, this Congress is laying down a new marker: the technology of the future—from semiconductors to batteries to electric vehicles—will be developed in America and made in America, by American workers.

It hasn't been easy, and our work is far from finished, but I'm optimistic.

I look forward to working with the Administration and my colleagues on this important issue.

PREPARED STATEMENT OF SENATOR PATRICK J. TOOMEY

Mr. Chairman, thank you.

China's economic and military rise poses the greatest challenge to core U.S. interests since the end of the Cold War. Under Xi Jinping's autocratic rule, China is seeking to dominate the Indo-Pacific, with clear security implications for U.S. allies and partners there, and engaging in relentless efforts to undermine human rights and American values, including free expression, the rule of law, and democratic governance.

Recently, White House officials and a few of my Senate colleagues have advanced a peculiar idea that in order to fully meet this challenge posed by China, the United States should adopt some of the Chinese Government's strategies for managing its economy. That thinking has led this Congress to enact industrial policy like new distortive taxpayer subsidies for semiconductor manufacturing. I thought that approach was a big mistake.

Especially given that recent episode, I am concerned about efforts to impose new capital controls on American investment in China. Advocates want a new regulatory regime so U.S. officials are notified of, and can potentially stop, U.S. investments in certain Chinese businesses.

If those investments credibly pose a risk to our national security, then I'm not reflexively opposed to this concept. However, there are several reasons why we should proceed carefully with this idea.

Some claim that current U.S. legal authorities, including our dual-use export control system overseen by the Bureau of Industry and Security, or BIS, are inadequate or incapable of addressing the risk posed by American investments in China. But it's important to remember that BIS regulates the flow of goods, software, and technology into jurisdictions and to end users of concern, and retains the force of law in the context of a U.S. investment.

As Commerce Undersecretary Alan Estevez told this Committee in July, BIS has complete authority to block the transfer, of any kind, of technology, intellectual property, blueprints, procedural know-how, or software going to China, including when Americans make investments in China. What, then, is the need for an outbound investment notification regime?

Well, in the words of National Security Advisor Jake Sullivan, it would capture outbound investments that "circumvent the spirit of export controls." It appears Mr. Sullivan was referring to certain U.S. investments in China that are legal under U.S. law, but might be of concern.

It appears that Mr. Sullivan's concern is investments that could result in the transfer of operational and managerial expertise and enhance the ability of Chinese firms to make sophisticated technologies might be prohibited from receiving if a U.S. company wanted to export those technologies. The inherent problem with Mr. Sullivan's invoking the "spirit of export controls" is it's hard to define a "spirit," and therefore, it could be subject to expansive and varying interpretation.

While I think we should carefully examine this issue, I'm concerned that the White House is reportedly rushing to issue an Executive order that establishes an outbound investment regime unilaterally. Let me be very, very clear about this: An Executive order is not a substitute for a new congressionally passed law. Legislation benefits from a deliberative, open, and democratic process.

A White House EO will inherently lack these characteristics—even if an EO is accompanied by a notice and comment period—and certainly should not precede a law. In addition, an EO will, very likely, place no limits on what technologies can be added to the regime in the future.

Why is it important to establish clear parameters on an outbound regime from the outset? Because time and again, presidents of both parties have misused sweeping national security authorities in ways far beyond how Congress initially intended. President Trump nearly used IEEPA to impose tariffs on Mexico over immigration policy. And Democrat and Republican senators were shocked when President Trump abused 232 “national security” authority to impose tariffs on U.S. partners and allies.

We should all be equally opposed to the Biden administration’s continuation of the Trump administration’s abuse of power under Section 232, which continues to this day. Appropriately scoping an outbound regime is important to preclude it from being used as a backdoor for trade protectionism in the future.

It’s vital that we prevail in this contest with China. We can do so by ensuring that the United States remains the single greatest global destination for capital formation, research and development, and the smartest minds in the world to come and work.

Creating a flawed outbound investment regime would undermine our economic leadership, discouraging the flow of capital, ideas, and people into the United States. After all, why would you start a firm in the U.S. if you know doing so risks precluding you from investing in China—the second largest economy in the world?

Given these stakes, I’m recommending a set of principles to guide the creation of any outbound investment regime. These principles are based on the premise that it is wholly irresponsible to have a regime that does not have clear statutory boundaries on its application. Therefore, a notification regime for outbound American investments in China should, at a maximum, only be applicable to direct U.S. investments in Chinese entities that are manufacturing, producing, developing, or testing a technology, for which a U.S. exporter would otherwise be required to seek a license under current U.S. law to export. I intend to solicit feedback on these principles, and work with Senators Cornyn, Casey, and Chairman Brown to incorporate them into the upcoming National Defense Authorization Act.

PREPARED STATEMENT OF SENATOR ROBERT P. CASEY, JR., OF PENNSYLVANIA

Thank you, Chairman Brown, Ranking Member Toomey, and Members of the Committee for inviting me to this important hearing today. I am pleased to have this chance to testify in support of an outbound investment screening mechanism. And I am grateful to Senator Cornyn for his partnership in this effort, as well as our colleagues in both the House and the Senate who are sponsors of the legislation, the National Critical Capabilities Defense Act (S. 1854), including Representatives Rosa DeLauro, Bill Pascrell, Brian Fitzpatrick, and Victoria Spartz.

For decades, the United States has steadily ceded its manufacturing power to other countries, particularly foreign adversaries, like the Chinese Communist Party (CCP) and the Russian Federation. Outsourcing our manufacturing and supply chains has put our economic and national security at risk. Unfortunately, the pandemic exacerbated this problem, as we experienced acute shortages of things like PPE and computer chips, simply because we were reliant on other countries to manufacture them and a broken supply chain to get them to us.

In 2020, during the COVID-19 pandemic, I first introduced the National Critical Capabilities Defense Act to require targeted Government screening of certain transactions by U.S. companies doing business in adversarial countries. This bill would help the U.S. better understand the risks of allowing foreign adversaries to gain access to critical capabilities and technology and to design and manufacture goods critical to our economic and national security interests. Over the past 2 years, we have garnered growing bipartisan and bicameral support for this concept, and Biden administration officials and key stakeholders have expressed support for an outbound investment screen, but we need more focus on this across the Government and Congress.

Without such a focus—without an outbound investment screening mechanism—we cannot understand, much less safeguard, critical domestic industries and capabilities for American workers, manufacturers and innovators. We must avoid aiding and abetting our economic competitors and potential adversaries.

At the heart of this is manufacturing, which is core to our economic competitiveness. In the United States, manufacturing represents about 11 percent of GDP, but is responsible for 70 percent of R&D, according to analysis from the consulting firm

McKinsey.¹ Manufacturing drives innovation. When you lose manufacturing, you lose innovation. Countries that don't make things don't endure.

Working men and women in Pennsylvania have seen the damage that decades of offshoring and the hollowing out of American manufacturing strength and knowledge does to communities and industries. Pennsylvania suffered record manufacturing job losses over the last generation. According to the Economic Policy Institute, China, governed by the CCP, cost the U.S. 3.7 million jobs between 2001 and 2018. 2.8 million jobs—three-fourths of the total jobs lost in this time period—were in manufacturing. 137,300 of those jobs were in Pennsylvania.² Jobs numbers alone provide little insight into the family and community trauma, as well as economic scarring, that have ravaged many small towns. In key sectors such as communications equipment, electronics and computer technology, we have ceded up to 40 percent to 60 percent of the domestic market share to Chinese imports, and globally the People's Republic of China (PRC) has captured extensive market shares in those sectors as well.³ We have learned from the intelligence community and law enforcement of the security risks that the loss of that production and those capabilities has fueled.

To add insult to injury, investments are being made in our rivals, such as the PRC and Russia. The level of U.S. investment in Chinese companies is staggering, which benefits the CCP. U.S. foreign direct investment has flooded into the PRC over the last three decades. Lately, U.S. firms have been targeting investments in high-tech and advanced service sectors. According to SEC data, in 2020, U.S. firms collectively invested in Chinese companies over \$200 billion in artificial intelligence, \$50 billion in biotech, and approximately \$80 billion in telecom, semiconductors and other technologies.⁴ In fact, many of these investments have been made in companies owned, controlled or influenced by the CCP. As of 2020, U.S. investments in PRC companies totaled by capital investment \$152 billion to Chinese State-owned enterprises and \$54 billion to Chinese military companies.⁵

But it's not just the investment dollars, it's the actual operations and capabilities that are being outsourced to the PRC. Research from the U.S.–China Economic & Security Review Commission, a bipartisan entity created by Congress, showed that, based on official U.S. data, the rate of R&D investments by some of our firms in the chemical and pharmaceutical sector in the PRC outpaced the rate of their domestic investments during the period examined almost three-fold.⁶ We have seen our growing reliance on the PRC for many of our life-saving and life-supporting drugs. We cannot afford to continue that dependence.

At present, the Executive and Legislative branches of our Government have little knowledge of where these dollars are going and what sort of projects they may be supporting once dollars are invested. They could very well be used against us or our allies in the future. We risk funding threats to our own national security and that of our allies. According to former U.S. National Security Adviser H.R. McMaster, venture capital firms are pouring billions into Chinese companies that are “developing dual-use and sensitive technologies that are going to be weaponized against us or already are aiding and abetting the Russians.” The National Critical Capabilities Defense Act would help us prevent such threats to our own security.

Outbound investment of this kind aids the CCP in its ongoing efforts to steal our technology for the benefit of its industries. Without a mechanism to understand the ways in which the export of U.S. investment and capabilities are resulting in a wholesale transfer of American R&D and expertise to our adversaries, the U.S. Government is an active party to the decline of our own economic might and national security.

¹Foroorhar, Rana, “Why Manufacturing Matters to Economic Superpowers”, *Financial Times* (April 11, 2021) <https://www.ft.com/content/22dd4058-c283-45c3-8877-8c2507ec7d6b>.

²Robert Scott and Zane Mokhiber, “Growing China Trade Deficit Cost 3.7 Million American Jobs Between 2001 and 2018”, Economic Policy Institute (Jan. 30, 2020), available at <https://www.epi.org/publication/growing-china-trade-deficits-costs-us-jobs/>.

³Robert Scott and Zane Mokhiber, “Growing China Trade Deficit Cost 3.7 Million American Jobs Between 2001 and 2018”, Economic Policy Institute (Jan. 30, 2020), available at <https://www.epi.org/publication/growing-china-trade-deficits-costs-us-jobs/>.

⁴Nikhaktar, Nazak, Testimony Before Senate Select Committee on Intelligence, Open Hearing: Countering the People's Republic of China's Economic and Technological Plan for Dominance, (May 11, 2022). <https://www.intelligence.senate.gov/sites/default/files/documents/os-nikhaktar-051122.pdf>

⁵Ibid.

⁶Malden, Kaj, and Listerud, Ann, “Trends in U.S. Multinational Enterprise Activity in China, 2000–2017”, U.S.–China Economic and Security Review Commission (July 1, 2020). <https://www.uscc.gov/sites/default/files/2020-06/US-Multinational-Enterprise-Activity-in-China.pdf>

The CCP has made clear over the past decade and more its willingness to sever access to critical supply chains and use economic coercion to bully other Nations. The CCP has acted on such threats. It has used market access as a weapon against one of our core security partners, Australia. In 2020, when Australia called for an independent inquiry into the origins of COVID-19, the PRC responded by slapping duties on Australian exports and revoking Australian producers export licenses. Last year, when Lithuania allowed the opening of a Taiwanese representative office in its capital of Vilnius, the PRC began a punishing campaign of economic coercion including market access and import restrictions. The PRC obstructed the export of rare earth materials to Japan as leverage to compel Japan to release the captain of a Chinese fishing boat who was detained after a boating accident in disputed water. There are countless other examples like these from around the world.

It's not hard to imagine a scenario where the PRC ceases the export of computer chips or critical rare metals to the U.S. or an ally, leaving us unable to respond due to a lack of domestic capacity or alternative means of procuring them. The U.S. must confront a Chinese regime determined to bully or steal its way to economic superiority.

Some critics have said that outbound investment screening should be left to the free market and private companies to sort out. The PRC and Russia will continue to ignore international law, as well as private, free market rules. Nazak Nikakhtar, in testimony before the Intelligence Committee earlier this year said as follows: "These are not incidental consequences of open and free trade. These are the very perverse and adverse consequences of one country exploiting open borders to cripple other Nations' economies. Our economic losses have resulted from the PRC's deliberate attempts to hollow out our industries in order to create dependency on their own distorted market."⁷

The PRC's broader military and governmental ambitions are intertwined with its trade and economic actions because the Chinese Government's agenda blurs the lines between its economic and defense sectors by way of its "civil-military fusion" approach. The Chinese Government's investment in, and theft of, technology and innovation supports the expansion of its security posture through development of surveillance technology, nuclear powered submarines and products across the commercial spectrum. This means the PRC does not view competition strictly through the lens of dollars and cents. When Chinese firms and State-sponsored enterprises compete against America's, it is done so with broader objectives in mind, including those of their military.

It is up to U.S. policymakers, not international markets, to be vigilant regarding our national security, our manufacturing capacity, and our workers.

We have existing authorities that already play an important role in preventing some transfer of technology and expertise but there are significant gaps that exist in our export control programs. The Export Control Reform Act (ECRA) expansion was a compromise reached during the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) debate. However, the ECRA expansion does not cover much of the goods and production that our bill focuses on. We need better oversight pertaining to supply chains, sourcing and investments that do not rise to the level of export control.

Today, we will hear testimony from Dr. Sarah Danzman, a Professor at Indiana University. In her recent paper on designing an outbound investment mechanism she acknowledges the gaps in export controls and has written as follows: "Export controls can regulate specific transfers of technology, but are not well suited to capture the full range of operational activities that relate to development of indigenous capacity and that may flow along with an investment. For example, running a successful semiconductor-fabrication plant that can produce quality chips at scale requires extensive management expertise and skilled leadership, in addition to the underlying technology and capital contribution. Export controls cannot constrain all of these factors, yet these are the exact types of contributions that would naturally flow into China's domestic sector by virtue of a U.S. investment."⁸

The focus of our NCCDA bill is foreign adversaries like the PRC and the Russian Federation. We need a specific outbound screening mechanism to prevent a foreign

⁷Nikhakhtar, Nazak, Testimony Before Senate Select Committee on Intelligence, Open Hearing: Countering the People's Republic of China's Economic and Technological Plan for Dominance, (May 11, 2022). <https://www.intelligence.senate.gov/sites/default/files/documents/os-nikhakhtar-051122.pdf>

⁸Danzman, Sarah, and Kilcrease, Emily, "Sand in the Silicon: Designing an Outbound Investment Controls Mechanism", (September 14, 2022). <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/sand-in-the-silicon-designing-an-outbound-investment-controls-mechanism/>

adversary from threatening access to critical capacities or supply chains. We do not need to screen every country, only adversaries and “countries of concern”.

Our legislation also recognizes the need for a multilateral approach with our partners and allies to ensure that we help them foster their development and implementation of similar, complementary mechanisms. In the long term, we need to expand coordination and diplomatic efforts to effectively confront the threats posed by our common foreign adversaries. The U.S. should align our own outbound investment review mechanism with those of allies and partners, such as South Korea and Taiwan, who have already taken this necessary step to protect their national security.

I want to thank the stakeholders and companies that over the past year have engaged with my office and our fellow cosponsors to offer constructive feedback and input to revise our legislation. We must put our Nation and its long-term national security and economic strength over short-term corporate profits. Our national security, our workers and our economic interests should never be sold out just for short-term gains. Americans across the political spectrum recognize the problem we are confronting and the need for a solution.

I want to commend the Biden administration for its support for our revised legislation and their efforts to advance an outbound investment screening mechanism. Commerce Secretary Gina Raimondo, United States Trade Representative Katherine Tai and National Security Council Advisor Jake Sullivan, have all publicly expressed support for our legislation.

I still believe our revised legislation provides the U.S. with the strongest path forward to compete in a global economy. American workers and our national security cannot afford to wait. Legislative action on this front is long overdue to address the scope and magnitude of the substantial risks we face as a country. This week, I sent a letter with Senator Cornyn, Majority Leader Schumer, Speaker Pelosi and Representatives DeLauro, Fitzpatrick, Pascrell, and Spartz to President Biden urging the Administration to move forward with Executive action to safeguard our national security and supply chain resiliency by screening outbound investments to foreign adversaries. We stand ready to learn how we can support the Administration’s proposals and shore up the resources the Administration will need to stand up such a mechanism.

An outbound investment screen is an idea whose time has come. We must move beyond examination to action because our national security, American workers and industry, can no longer wait.

Thank you for your time and consideration.

PREPARED STATEMENT OF SENATOR JOHN CORNYN OF TEXAS

Thank you Chairman Brown and Ranking Member Toomey for organizing this hearing on such an important and timely topic.

As many of you know, China poses a vast threat to our national security.

Nearly 20 years ago, our Government opened the door to do business in China and our industry did what they do best—found a market, captured it, and achieved efficiency and innovation.

But it didn’t take long before that openness was abused by the Chinese Communist Party through theft, control, and perversion.

Now, we’re seeing the vulnerabilities created by the open door between our economies.

The Chinese Communist Party has weaponized our trade and financial apparatuses and is using them to achieve control, dominance, and self-sufficiency in the area of our national critical capabilities.

This includes technologies such as semiconductors, quantum computing, and artificial intelligence.

Following passage of the CHIPS act, the U.S. is the only allied, Pacific Nation that provides domestic semiconductor incentives and does not have an outbound investment mechanism.

The CCP’s predatory trade practices paint an alarming picture for our national security.

This requires a collective response by the U.S. Government, American businesses, our allies, and those Nations who at least attempt to abide by the rules-based international trading system.

That said, we must not overreach. Trade and investment with China must continue, so any legislative or regulatory actions must be targeted.

We need a scalpel, not a sword.

The first step is to improve visibility into human, financial, and intellectual capital in foreign adversary Nations. We must know the full extent of the problem.

I support a robust process that focuses on transparency and notification. The American people should know if a company is investing in critical industries on a foreign adversary's soil.

For example, if a U.S.-headquartered company chooses to finance AI software for the People's Liberation Army, it is actively investing in China's military strength.

In the event of a conflict with Taiwan or worse, our own men and women in uniform, China would have a military advantage that was funded in part by an American company.

I'd like to note that this is not a hypothetical example—this happened. That's why this is so critical.

There's an old saying attributed to Vladimir Lenin. "The capitalists will sell us the rope with which we will hang them."

That's exactly what China is trying to do—use the enterprising minds of America to choke our economy.

The challenge we face with regards to China in particular requires a shift in our way of thinking—a new paradigm. The focus on proxy wars and diplomacy are a relic of the past. We need real action.

That said, our Government cannot risk playing politics with an important topic like outbound investment to settle a centuries-old debate over protectionism versus free trade or labor vs big corporations.

And we must act soon, or we risk policy being made on the campaign trail.

I know that I am not alone, and I speak for many of my colleagues who understand the grave national security risks.

The perspectives of the members of this panel, especially my good friend and Ranking Member Toomey, are necessary in us finding balance.

I thank the Chair and Ranking Member for inviting me here today to set the scene for today's hearing.

I also want to thank my colleague Senator Casey for being a productive partner in this effort.

I hope it is one of several hearings to come that will provide additional, diverse perspectives and oversight on the topic.

PREPARED STATEMENT OF SARAH BAUERLE DANZMAN
ASSOCIATE PROFESSOR OF INTERNATIONAL STUDIES, INDIANA UNIVERSITY

SEPTEMBER 29, 2022

Thank you, Chairman Brown and Ranking Member Toomey as well as your hard-working staff for inviting me to testify on outbound investment, its implications for national security, and factors to consider if Congress decides to move forward with legislative proposals around screening or controlling such investments. It is an honor to speak with the Committee today.

Let me clarify from the outset that the views expressed in my testimony today are my own, and do not necessarily reflect the view of my employer, Indiana University, or of the Atlantic Council, where I am a nonresident fellow.

I speak today as someone with both an academic and a Government background. I am an associate professor of international studies at the Hamilton Lugar School at Indiana University. My research expertise includes the politics of investment liberalization, investment attraction, and the intersection of national security and investment policy, most notably inbound investment screening.

As a Council on Foreign Relations International Affairs Fellow, I worked as a policy advisor and CFIUS staffer in the Office of Investment Affairs at the Department of State from August 2019 to August 2020.

And, in my capacity as a fellow at the Atlantic Council I have had the distinct pleasure of coleading a policy working group on outbound investment controls with Emily Kilcrease of the Center for New American Security. Emily and I recently published a policy brief where we lay out our suggestions for how to design an outbound screening mechanism. Much of my comments today draw directly from that coauthored report.

The point of today's hearing is to take a step back from tactical issues of policy design to instead:

1. Lay out the potential national security risks that outbound investment may engender,
2. Identify existing gaps in U.S. authorities to adequately address these risks, and

3. Develop overarching principles to guide the development of any additional authorities related to outbound investment controls that the USG, including Congress, may pursue.

The central guiding point of my testimony is this: While there are a set of national security risks that some kinds of outbound investments generate, there remains a great deal of uncertainty about the size of the problem and the cost of potential solutions. Given that the openness of the U.S. economy has been a major driver in our prominent position in the global innovation economy and therefore our national security, any attempt at addressing the risks of outbound investment must equally consider the potential unintended consequences of action. Smart policy will be narrowly scoped to national security, rooted in fact, tailored to the technologies of greatest concern, mindful of the limits of de facto enforcement power, nonduplicative of existing tools, and attuned to the need to act multilaterally. This is not to say that controls are not desirable or feasible, but that any action should be carefully measured.

I want to use the remainder of my time this morning to offer five observations that Congress should keep in mind while contemplating outbound investment controls.

First, there are gaps in the United States' ability to address national security risks associated with some kinds of outbound investment. Export controls can stop the flow of U.S. technology to these activities. But active forms of U.S. investment—particularly foreign direct investment (FDI) and venture capital (VC) can provide intangible benefits to the Chinese firms and industries in which they invest. The United States can cut off all economic activity between U.S. persons and problematic entities through list-based sanctions programs. However, there are reasonable arguments for why narrowly scoped expanded review authorities are necessary to protect national security.

Second, Congress should resist temptations to use outbound investment screening for purposes other than national security. The United States has national and economic security interests that intersect, and sometimes conflict, with the outbound investment activities of U.S. multinationals and investors in several respects. To be consistent with a broader and long-standing commitment to market openness, the authority to intervene in an outbound transaction must be limited to a fact-based national security risk assessment, as is the case with inbound investment through the CFIUS process. It is my assessment that any outbound screen should focus on national security risks associated with indigenous technology development in countries of concern.

Third, Congress should recognize the uncertainty that pervades this issue. Crucially, current data collection on U.S. investment flows to China is not detailed enough to be able to assess the national security implications of individual transactions. This is one reason why I advocate for a notification regime to help scope the size of the problem. An Executive order related to outbound screening is likely a good first step because it allows for more experimentation before committing to a statutory requirement. This mirrors the experience of CFIUS, which was first established through Executive order in 1975 and gradually became a statutory requirement through a series of amendments to the Defense Production Act, starting in 1988.

Fourth, Congress should not assume that a mirror image of CFIUS will work for outbound screening. The enforcement issues associated with regulating the movement of investment abroad is more challenging to address than regulating inbound flows. In the CFIUS case, a prohibition is enforced by preventing a foreign entity from buying a domestic asset, which is subject to U.S. regulation. For outbound transactions, the United States can impose penalties on the U.S. entity implicated in the transaction. But enforcement options become much less palatable if a multinational decides to channel the otherwise prohibited investment through a third country. It is also easier to compel a U.S. target of a CFIUS review to provide the Committee with the sensitive nonpublic technical information often required to complete a risk analysis. Compelling similar information revelation from a foreign target in the context of an outbound review will be much harder. The PRC might simply prohibit the transfer of such information.

Congress should be clear-eyed about the compliance and enforcement challenges likely to arise from outbound investment review that are less problematic in the context of inbound review. It should only move forward with a screening concept if it is reasonably sure that it has adequate monitoring and enforcement capabilities to give the regulation teeth.

Finally, Congress should think in network terms when contemplating what technologies to work hardest to protect. An administrable outbound investment review

system will need to be relatively narrow in scope. We should avoid a “boiling the ocean” mentality. A broadly scoped review is likely to generate substantial negative consequences for U.S. companies’ competitiveness and capacity to innovate. Congress can narrow its focus while remaining maximally effective by examining technology chokepoints in supply chain networks where U.S. firms currently have the advantage and where process and know-how are central to the production of these technologies. A recent Center for Security and Emerging Technology report mapped China’s technology chokepoints. It found that the technologies for which China has the least domestic capacity tend to be in areas with very high quality control specifications. These kinds of technologies are likely of high national security value, require substantial know-how to perfect, and have outsized follow-on effects to other technologies relevant to U.S. national security. They are good candidates for review.

At the same time, the United States’ ability to leverage its network position depends on China being integrated to some degree into the technology network. Congress should be mindful to not control technology and outward investment so much as to push China out of the network entirely. Take semiconductors as an example. The sanctions alliance against Russia’s invasion of Ukraine has been highly effective at cutting off Russia’s access to advanced semiconductors. As National Security Advisor Sullivan recently stated, this has substantially degraded the Russian military’s capabilities.¹ However, if Chinese entities could fabricate advanced semiconductors without access to U.S. and other alliance members’ technology, we would lose this powerful tool. Right now, many Chinese companies seem to prefer to use U.S. technology rather than invest the capital and time necessary to develop their own solutions. But, if we cut them off from this technology entirely, or if we develop policies that create enough uncertainty about future access, they will have no choice but to develop critical technologies domestically.

Prudent policy must balance the national security imperative to deny countries of concern indigenous capabilities in technology of high national security import, while also avoiding an overly restrictive regime that would inadvertently further push Chinese entities toward self-sufficiency.

U.S. Investment in China

To determine the size of the problem, we must first gather basic facts about how much U.S. investors are active in China, through what vehicles, in what industries and for what purposes. According to surveys of the Bureau of Economic Analysis’s surveys of U.S. Multinational Corporations activities abroad, U.S. companies have accumulated about \$118 billion in foreign direct investment positions in China.² This equates to about 1.8 percent of all U.S. FDI abroad. For comparison, 61.4 percent of all U.S. FDI abroad is located in Europe. Measurement of U.S. assets abroad, rather than FDI positions, suggest U.S. multinationals have roughly \$779 billion in assets in China.³ U.S. venture capital, which is usually not included in FDI figures, has invested about \$60 billion into Chinese start ups since 2010. To place this figure in context, venture capital activity in the United States over the same period was roughly \$1.28 trillion.⁴

These numbers suggest that U.S. investment in China remains relatively small compared to U.S. investment activity at home and also compared to U.S. investors’ activity overseas. Other argue, however, that evaluating the risks of such investment into China also requires attention to trends and to the specific activities to which U.S. investors are contributing. On the first point, all measures of U.S. investor activity suggest direct forms of U.S. investment into China peaked between 2015–2018 and have declined since then. The second point is harder to address given the data that are currently available. Data on sector specific investments provide some relevant information. U.S. investments in theme parks, real estate, and consumer retail are not likely to have substantial deleterious effects on national security. Investments in some information communication technology businesses and activities—which was the sector that received the largest share of U.S. FDI in recent years—could have security implications. But even sectors are too aggregated of a level of analysis to determine national security concerns. For example, investment in an enterprise software company serving the China market and investment

¹ <https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/09/16/remarks-by-national-security-advisor-jake-sullivan-at-the-special-competitive-studies-project-global-emerging-technologies-summit/>

² See <https://www.bea.gov/sites/default/files/2022-07/dici0722.pdf>.

³ Thilo Hanemann, Mark Witzke, Charlie Vest, Lauren Dudley, and Ryan Featherston. 2022. “Two Way Street—An Outbound Investment Screening Regime for the United States?” Rhodium Group. January, P. 15. Download here: <https://rhg.com/research/tws-outbound/>

⁴ Data from Pitchbook. Download here <https://www.statista.com/statistics/277501/venture-capital-amount-invested-in-the-united-states-since-1995/>.

in advanced semiconductor research and development likely have very different national security implications.

In other words, whether U.S. investment in China poses national security concerns is best analyzed at the level of transaction, item, or activity rather than by aggregated investment values. And, currently available data do not provide enough insight to adequately judge the potential national security consequences of these investments because they do not provide detailed enough information about the activities of the investment target.

Defining Policy Objectives of a Potential Outbound Screening Mechanism

The United States has national and economic security interests that intersect, and sometimes conflict, with the outbound investment activities of U.S. multinationals and investors in several respects. These include to prevent U.S. capital from supporting firms implicated in China's systemic abuse of human rights, to enhance the resiliency of critical U.S. supply chains, and to address concerns arising from China's indigenous development of technologies relevant to U.S. national security.

At the same time, an open, market-based economy remains a key source of economic and technological strength of the United States. The fungibility of capital and the global mobility of firms limits the ability of unilateral U.S. actions to prevent capital, knowledge, and technological flows to countries of concern. Policy action in this space needs to balance justifiable national security restrictions with a broad commitment to an open, market-based economy that seeds and sustains technological innovation. Bureaucratically complex and resource-intensive authorities are likely to have negative effects on competitiveness and could encourage the most innovative and productive businesses to relocate to less restrictive jurisdictions. Authorities that are too broad or ambiguous may have the same effect. Additionally, rules that do not have clear enforcement mechanisms for noncompliance will be of limited value.

The United States should limit any outbound control measures to national security—rather than broader economic competition—policy objectives. Furthermore, it should focus attention at the nexus of the most pressing national security concerns and the areas where interventions are most likely to successfully impede the most problematic policy objectives of countries of concern. This entails strengthening existing authorities before creating new ones and finding opportunities to pursue multilateral coordination or action with allies and partners wherever possible. National concerns related to China's indigenous technology development are those that can be most directly addressed through an outbound investment mechanism and represent a genuine gap in existing authorities. Human rights concerns and issues of supply chain resiliency are best addressed through other measures.

Human Rights

The United States has several existing tools that can be used to address concerns related to the use of U.S. capital or technology in facilitating human rights abuses. First, it can use the Non-Specially Designated Nationals Chinese Military-Industrial Complex Companies List (SN-CMIC) sanctions program to prevent U.S. capital from contributing to Chinese companies operating in the surveillance technology or defense and related materiel sectors. Second, export controls—via the Entity List or other means—can effectively stop the flow of U.S. technology to these activities, especially if the Export Control Reform Act of 2018 (ECRA) is amended to expand a prohibition on U.S. persons from providing support to a “foreign military, security, or intelligence services.”⁵ The Uyghur Forced Labor Prevention Act is another example of authorities Congress and the Executive branch can use to address similar concerns.

Supply Chains

Recent legislative efforts have coalesced around supply chain resiliency issues, which is not surprising in the context of COVID-19 and related supply chain disruptions. However, outbound investment screening is a poor tool for addressing supply chain restructuring. Because so much of the U.S. supply chain is already offshore, policies addressing supply chain security must focus on how to move operations already in countries of concern back to the United States or onward to partners and allies. Blocking a proposed outbound investment on reshoring grounds would not provide the company attempting to offshore with the capability to succeed in the

⁵ Currently, the ECRA language prohibits U.S. persons from supporting “foreign military intelligence services.” Rep. Malinowski (NJ) has proposed this targeted change in language.

United States on commercially viable terms. In other words, screening would only address a symptom rather than the cause of offshoring.

Moreover, using outbound screening to address supply chain resiliency is likely to generate problematic legal issues as well as complicate economic and security cooperation with our partners and allies. Blocking a proposed outbound investment on issues of supply chain resiliency would require either: (a) an outbound review mechanism to provide the President with the authority to block a transaction for reasons beyond national security, or (b) a further expansion of the concept of national security in ways that would damage the United States' reputation as an excellent place to start and grow innovative companies.

Expanding blocking rationale beyond national security would likely invite increased litigation from U.S. firms subject to an investment prohibition. CFIUS largely avoids such litigation because courts provide the President with substantial deference in the area of national security. Prohibitions on other grounds will likely be easier to challenge in court, and could create lengthy and costly legal battles that would increase regulatory uncertainty, thereby reducing the United States' status as one of the most desirable places to do business.

Further expanding the concept of national security also has important negative consequences. The first has to do with perceived legitimacy of U.S. Government action. While the public and industry mostly recognize the right of the U.S. Government to intervene in market activity that generates clear risks to national security, this support rests on common understandings of what is a reasonable claim to national security. Overuse of national security rationales to justify Government intervention into private sector transactions decreases the public's trust in the reasonableness of these claims. Eroding trust could lead to reduced voluntary compliance with the law, more creative work-around solutions, and a U.S. public that is increasingly skeptical of U.S. actions in the area of national security and economic policy.

Whatever the United States does with respect to outbound screening, we should be prepared for other countries to develop similar authorities. Outbound mechanisms focused on supply chain structures as an essential security issue and/or an economic resiliency issue that warrants prohibitory intervention could be used among our European allies and others in ways that would create substantial harm to U.S. interests, including by making it harder to develop more redundancy and multiple suppliers in critical supply chains through increased ties with allies' economies.

Establishing more resilient supply chains requires an affirmative industrial policy that addresses the root economic causes of offshoring of critical capabilities long before a company enters an offshoring transaction and that makes reshoring production commercially viable. In this regard, the incentives and other "run faster" provisions of the CHIPS and Science Act of 2022 are an excellent start. Attempts to reshape supply chains must also consider how to do so without creating additional negative supply shocks. These considerations are particularly important in the current context of high inflation that has been largely driven by supply-side shocks.

Impeding Chinese Indigenous Technology Development

Concerns over how U.S. technology and investment can support indigenous technology development in China was central to the policy discussion surrounding the 2018 reforms of CFIUS and export control authorities, through the Foreign Investment Risk Review Modernization Act (FIRRMA) and ECRA. The initial draft of FIRRMA provided CFIUS with review authority over outbound investments. Some lawmakers were especially worried that the PRC was benefitting from critical technology transfer from U.S. firms to Chinese counterparts through joint ventures. After substantial debate, Congress found a compromise in which CFIUS would remain focused on inbound—though it does have jurisdiction over some forms of outbound joint ventures—while national security concerns related to outbound investment would be regulated through expanded export control authorities.

The gap in this approach is that there are ways in which the participation of U.S. multinationals and investors in China's innovation economy can harm U.S. interests through channels other than technology transfer. Decades of research on the role of foreign direct investment in development has shown that inward FDI, particularly when paired with active host country regulatory strategies, can help FDI-receiving countries expand domestic markets and move up the value chain.⁶ Multi-

⁶The research on horizontal and vertical spillovers from inward FDI is vast. See, in particular: Christine Zhenwei Qiang, Yan Liu, and Victor Steenbergen. 2021. "An Investment Perspective on Global Value Chains". Washington, DC: The World Bank Group; Tomas Havranek and Zuzana Irsova. 2011. "Estimating Vertical Spillovers From FDI: Why Results Vary and What the True Effect Is". *Journal of International Economics* 85: 234–244. Zuzana Irsova and

national corporations and their affiliates make up 36 percent of global output and are responsible for two-thirds of exports and one-half of imports.⁷ Domestic firms participate in global supply chains largely through incorporation into MNCs supply chain. For instance, MNCs operating in the United States source 25 percent of their inputs domestically. MNCs in Japan source over 50 percent of inputs domestically. The more domestic firms interact with MNCs, the more they learn from those MNC, including how to increase their production capabilities. By interacting with MNCs, domestic firms gain foreign market knowledge to directly compete in international markets. Domestic firms that integrate into MNCs' supply chains are statistically significantly more likely to become exporters, increase their ability to supply the domestic market, and produce higher quality and more complex products. Normally, we view all of these spillover effects of FDI as beneficial to economic development. However, in narrow cases related to specific critical technologies relevant to national security, the linkages literature provides insight into how U.S. MNCs can help develop Chinese critical industries. The issue goes beyond technology transfer. MNCs help foster indigenous industries by incorporating local firms into their supply chains and by importing knowledge about international markets, connections to MNCs' broader supplier and buyer networks, and other managerial practices that increase efficiency and quality control. These, less tangible, contributions to the domestic market are not able to be controlled through export controls.

In the realm of U.S. venture capital (VC), there are also potential concerns that are not addressable through export controls. As the National Venture Capital Association (NVCA) lays out in their 2022 Yearbook, venture is distinct from other types of investing because it typically entails relatively small equity stakes in a company, but the general partner in the investment is much more involved in strategic management decisions of the target than passive investors are.⁸ VCs provide more than an infusion of capital; they mentor and advise founders who often need substantial strategic and logistical help to scale up their business. They often play prominent roles on corporate boards. Moreover, they provide founders and their teams with access to the investors' financial, commercial, professional, and political networks. By investing in a company, VCs are putting their seal of approval on the enterprise, signaling that the company was able to pass a thorough vetting process. And, when VCs invest in a company, they are tying their financial future to the company. It is in a VC's interest to crowd in more investors into future funding rounds so that the companies in which they invested increase in value in each funding round, which ultimately leads to an acquisition or initial public offering through which the VC can exit the investment, hopefully at great profit.

Venture Capital plays a critical role in the continued dynamism of the U.S. innovation economy. From 1974–2015, 42 percent of U.S. companies that went public were venture backed.⁹ These 556 companies accounted for 63 percent of the market capitalization of the 1,339 U.S. companies that went public over the period and 85 percent of all the research and development expenditures associated with those companies. The flip side, however, is that these same features that have been so central to the journey from start up to commercial viability in the United States could generate national security risks if U.S. VC contributes to critical technology start-ups in countries of concern. Similarly, to the intangible benefits of FDI described above, export controls do not provide an adequate remedy to these kinds of national security concerns.

Approaching Outbound Controls

As the Congress moves forward with an outbound screening concept tailored to issues of the national security risk of indigenous technology development in countries of concern, it should: (1) be mindful of dynamics that make outbound investment screening harder to enforce than inbound review, (2) measure potential tools

Tomas Havranek. 2013. "Determinants of Horizontal Spillovers From FDI: Evidence From a Large Meta-Analysis". *World Development* 42: 1–15; Sonal S. Pandya. 2016. "Political Economy of Foreign Direct Investment: Globalized Production in the Twenty-First Century", *Annual Review of Political Science* 19: 455–475; Sarah Bauerle Danzman. 2019. "Merging Interests: When Domestic Firms Shape FDI Policy". Cambridge University Press.

⁷The figures in this paragraph come from Qiang, Liu, and Steenbergen. 2021. "An Investment Perspective on Global Value Chains", The World Bank Group. See especially pp. 8, 10–13.

⁸National Venture Capital Association. 2022. NVCA 2022 Yearbook. <https://nvca.org/wp-content/uploads/2022/03/NVCA-2022-Yearbook-Final.pdf>, p. 10.

⁹Will Gornall and Ilya A. Strebulaev. 2015. "The Economic Impact of Venture Capital: Evidence From Public Companies", Stanford University Graduate School of Business Research Paper No. 15-55. Available at SSRN: <https://ssrn.com/abstract=2681841> or <http://dx.doi.org/10.2139/ssrn.2681841>.

against five principles of good design, and (3) follow a strategy that leverages the United States' privileged position in many technology supply chain networks.

Enforcing Outbound Screening

The conversation around outbound screening is colored by the United States experience with inbound review. CFIUS is widely seen as well-designed and effective and Congress should be careful to not overlearn from the CFIUS example. It is much easier from an enforcement perspective to control market access than to limit outflows. In the CFIUS case, a prohibition is enforced by preventing a foreign entity from buying a domestic asset, which is subject to U.S. regulation. For outbound transactions, the United States can impose penalties on the domestic entity implicated in the transaction. But enforcement options become much less palatable if a multinational decides to channel the otherwise prohibited investment through a third country. Enforcing a prohibition in that case would likely require substantial extraterritorial reach that the U.S. Government will likely wish to avoid due to issues of proportionality and allies' and partners' sensitivities.

Other aspects of administration and enforcement are much easier for inbound investment than for outbound. For instance, it is easier to compel a U.S. target of a CFIUS review to provide the Committee with the sensitive nonpublic technical information often required to complete their review than it would be to compel the same information from a foreign target in the context of an outbound review. Indeed, other country Government may simply prevent the foreign target from providing such information. Additionally, in the case of mitigation agreements, it is reasonable to assume it is much easier for the U.S. Government to monitor behavior of firms in own jurisdiction than firms overseas.

For these reasons, Congress should be clear-eyed about the compliance and enforcement challenges likely to arise from outbound investment review that are less problematic in the context of inbound review. Congress should only move forward with a screening concept if it is reasonably sure that it has adequate monitoring and enforcement capabilities to give the regulation teeth.

Design Principles

Along with having enforcement capabilities strong enough to deter, Congress should consider the following principles when designing a screening tool.

1. Review should be targeted to transactions that present the highest national security threat and any governmental action should be subject to a national security risk assessment. As with CFIUS, an outbound mechanism should be narrowly tailored to national security risks rather than a tool to bolster broader economic competitiveness objectives. Congress should instead pursue issues of competitiveness and social standards through affirmative industrial policy such as the CHIPS and Science Act and through trade and investment frameworks such as the Indo Pacific Economic Framework (IPEF).
2. A review mechanism along with any additional outbound controls should be clearly defined and understandable to private-sector participants. This includes clear definitions of what types of investors and economic activities are covered. The private sector will be responsible for the first line of compliance, so they must understand to what they are obligated. For the regulation to be seen as a legitimate use of the Government's regulatory authority, its purpose and necessity must be explainable to the American public. Without public support, firms will not face substantial reputational costs for evading the spirit or the letter of the regulation. A supportive public is key to regulatory compliance.
3. Any review should be nonduplicative of existing tools such as export controls. In the context of inbound transactions, CFIUS is designed as a tool of last resort. Any outbound investment screen should be thought of similarly and any use of outbound authorities should occur only when other authorities are insufficient to address the national security risk that arises from the transaction in question.
4. Any review mechanism must be scoped proportionately to the Government's institutional capacity to effectively administer a new mechanism. We should not take lightly the administrative burden that a well-functioning outbound review process would place on the Executive branch. For example, CFIUS requires hundreds of staff and attention across its nine member agencies plus ex officio and support agencies. FIRRMA appropriated \$20 million a year for 5 years to help build up CFIUS agencies to support the expansion of its authorities.
5. Finally, any Congressional action on outbound screening should be paired with meaningful multilateral engagement with allies and partners so that U.S. investors are not disadvantaged and so the goal of impeding national security

relevant indigenous technology development in countries of concern is more likely to be met. Similar to export controls and inbound screening, outbound investment controls are more likely to be effective if large portions of the global economy implement similar measures. This is especially important in the context of outbound investment where there is justifiable concern that a U.S. outbound mechanism without coordination with other advanced economies could just lead to MNCs from other OECD countries occupying the investments that U.S. firms otherwise would have participated in. Similarly, multilateral engagement is important in the context of critical technologies, as the United States is not the only relevant member of these supply chains.

Leveraging the U.S. Network Position

As a final conceptual point, I encourage Congress to think in network terms as much as possible when contemplating any outbound investment control mechanisms. Even before the COVID-19 pandemic, scholars of International Relations started to borrow from complexity science to understand on the structure of different kinds of global networks generate power and vulnerabilities. The United States has effectively leveraged its central position in currency and finance networks to extend its power in important ways. Even now, we see how this centrality has imbued the United States with regulatory power over companies that wish to list on U.S.-based exchanges.

As the Congress shifts from conceptual issues to more tactical and technical concerns related to coverage and definitions, I encourage it to use insights from complexity science to design its mechanism. This entails focusing attention on chokepoint technologies as much as possible. Rather than trying to “boil the ocean” and cover all technologies possible, it will likely be more effective for the U.S. to evaluate what specific technologies are especially critical to a host of other technologies. For instance, it may be particularly challenging to cover all manner of Artificial Intelligence technologies. However, limiting investment in specific extreme ultraviolet lithography tools and technology as well as most likely candidates for the next next-generation lithography may be more feasible. To the extent that advanced AI relies on advanced semiconductors, controls on NGL will have spillover implications for AI as well.

As another example, the Center for Security and Emerging Technology recently published a report evaluating “China’s Self-Identified Strategic Technology Import Dependencies”.¹⁰ It found that China’s chokepoints tend to be in technologies with very high-quality control specifications including precision requirements, consistency requirements, and the ability to perform under stress. Focusing attention on these areas—or more broadly, areas that the Chinese self-identify as chokepoints—would likely be particularly because these chokepoints relate to production process issues rather than the underlying technologies. Additionally, research on information problems in authoritarian contexts suggest that achieving high levels of quality control will likely remain a challenge for Chinese companies so long as delivering bad news is politically dangerous. This suggests not only that the PRC currently faces disadvantages in these chokepoint technologies, but also that the United States’ open, democratic system provides us with a clear competitive edge in these areas. This is an important reminder that the United States’ leadership position in advanced technology and economic dynamism is a function of our open, non-arbitrary, rules-based system. To best protect our national security, we should confidently embrace those core principles that have fueled our economic prosperity rather than erect overly complicated bureaucratic structures that emulate competitors’ systems.

Conclusion

I close my testimony where I began. Outbound investment creates a range of policy issues that Congress may want to address. The issue is which issues warrant a policy response and, of those, what policy response, or combination of policy responses, is most likely to produce outcomes that strengthen U.S. national security.

I recommend that Congress consider five issues while contemplating the path forward:

First, the gaps that currently exist in the Government’s authorities relate to the ability to control the intangible benefits associated with outbound FDI and VC flows. Export controls already provide authority over technology transfer. Policy solutions will need to address the components of investment that generate risks

¹⁰ Ben Murphy. 2022. “Chokepoints: China’s Self-Identified Strategic Technology Import Dependencies”. Center for Security and Emerging Technology. Available here: <https://cset.georgetown.edu/publication/chokepoints/>.

through managerial expertise, transfer of know-how, connection with supplier and buyer networks, and the legitimation effects of partnering with a U.S. investor.

Second, any outbound investment review mechanisms should be narrowly focused on national security rather than broader policy objectives. Issues of economic competitiveness are best addressed through other tools.

Third, outbound investment screening would be a new authority and represent a substantial break from central tenets of decades of U.S. economic policy. There is a great deal of uncertainty about the size of the problem and the potential negative unintended consequences of outbound review. An approach that is designed to gather more information as well as allow for experimentation is likely to work better than enacting a broad statutory screening requirement all at once.

Fourth, Congress should not assume that a mirror image of CFIUS will work for outbound screening. The enforcement issues associated with regulating the movement of investment abroad is in many ways more challenging to address than regulating inbound flows. Congress should make sure that any mechanism be narrowly scoped to national security, clearly defined and seen as a legitimate use of Government authorities, nonduplicative of existing tools, administrable, and paired with meaningful multilateral engagement on the issue with allies and partners.

Finally, smart policy will take cues from networks and complexity science. Clamping down on all outbound investment to countries of concern is not a viable option. By focusing on chokepoint technologies, the United States can scope coverage in a way that is most impactful with the least amount of negative economic consequences.

PREPARED STATEMENT OF RICHARD ASHOOH

FORMER ASSISTANT SECRETARY FOR EXPORT ADMINISTRATION, U.S. DEPARTMENT OF COMMERCE

SEPTEMBER 29, 2022

Chairman Brown, Ranking Member Toomey, and Members of the Committee, thank you for the opportunity to testify before you today. Today's hearing is a timely, relevant, and critical examination of the issues associated with U.S. originated investments to countries, companies, or causes which may pose a national security threat or otherwise threaten U.S. interests. Having served as Assistant Secretary of Commerce for Export Administration at the Bureau of Industry and Security (BIS) in the prior Administration from 2017 until 2020, I had both the honor and challenge of weighing many of these very issues, especially with respect to concerns over unauthorized technology transfers as the primary purview of the Bureau. It is in that capacity that I am testifying here today. In short, I understand the difficulties the Committee and Congress face in the effort to implement effective policies and hope my participation today constructively contributes to that goal.

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 is never static and must be constantly addressed.

Much of what has been accomplished in recent years is the result of legislation this Committee championed in 2018 which led to the Export Control Reform Act and Foreign Investment Risk and Review Modernization Act, also known as ECRA and FIRRMA. That debate considered many of the issues captured by today's review of the need for enhanced scrutiny and action regarding outbound investments and has many lessons to offer policymakers. At this point, I would like to underscore my gratitude to the Committee for the thoughtful approach it took at that time, which involved bipartisan, bicameral, and multijurisdictional legislating to advance a long-overdue modernization of some very complex and powerful authorities. Any consideration of measures which could significantly alter U.S. capital flows merits, in my view, a similarly thoughtful and thorough approach.

While the issues associated with regulating financial behaviors to obtain a national interest objective are many, I will confine my comments today to three recommendations that are drawn from the lessons learned in the consideration and implementation of FIRRMA and ECRA.

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—thanks to the concomitant updating of that law with FIRRMA.

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. This synchronization—further refined in regulation after FIRRMA and ECRA passed—is a model for enhancing the power and effectiveness of U.S. Government policy implementation.

Recommendation: Outbound screening criteria should align with the criteria that is already the foundation of the export licensing and in-bound investment authorities.

3. *Build on what works.* 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. Again, using the ECRA/FIRRMA example, the amendments allowed the two regimes to reinforce each other as complementary tools to protect national security. 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.

Recommendation: Congress should consider whether existing authorities such as the export control system can be leveraged as a tool to obtain insights into financial transactions of concern, or even address gaps in the current system.

As I said at the outset, these concerns are real and gaps in the system pertaining to financial transaction merit immediate attention. As the principles I have discussed here illustrate, it is my view that amendments to current authorities hold the potential to address the most pressing concerns regarding outbound investments, without the establishment of an additional, entirely new regime.

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, some consideration 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.

I am happy to take your questions.

PREPARED STATEMENT OF THOMAS FEDDO

FORMER ASSISTANT SECRETARY FOR INVESTMENT SECURITY, U.S. DEPARTMENT OF
THE TREASURY

SEPTEMBER 29, 2022

Chairman Brown, Ranking Member Toomey, and distinguished Members of the Committee, I am honored to appear before you today, and to join my fellow witnesses in this important discussion.

When I last appeared before the Committee, I was fortunate to receive its endorsement to be the Treasury Department's first-ever Assistant Secretary for Investment Security. In that role, I led and oversaw the operations of the Committee on Foreign Investment in the United States (CFIUS), including the timely and successful implementation of its historic overhaul after enactment of the overwhelmingly bipartisan Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA).

By virtue of that experience, and the benefit of roughly 27 years of Government service—more than two decades in national security-related capacities—I hope to contribute to your consideration of so-called “outbound” investment screening and whether such a tool should be implemented.

At the outset, I will say that I believe we are engaged in one of history's most consequential great power competitions, and that technology plays a key role in that contest. Leaders of both the current and prior Administrations have warned of the existential challenge posed by the People's Republic of China (PRC) and its policy of “civil-military fusion”—exploiting corporate advancements and innovation in technology to close the battlefield gap. Secretary Michael Pompeo's State Department noted that civil-military fusion “aims to make any technology accessible to anyone under the PRC's jurisdiction available to support the regime's ambitions.” And Secretary of State Antony Blinken has described Beijing's intent as: “to spy, to hack, to steal technology and know-how to advance its military innovation and entrench its surveillance State.”

In the 1990s, I served as an officer on a Los Angeles class nuclear-powered fast-attack submarine. That boat was, as are today's generation of U.S. submarines, a technological marvel; a “black hole” in the deep, carrying the world's most sophisticated weapons and equipment. This is in great part a result of America's innovation ecosystem, both in and outside of the defense industrial base. Having first-hand experience in that submarine environment, the imperative for maintaining America's technology advantage is crystal clear to me—it promotes the capability to win decisively on the battlefield, whether under or on the sea, on land, or in the air, space, or cyber domains.

The PRC poses grave threats to the United States and its allies and to the global world order; including its strategy to exploit technology, raw materials, market power, and energy resources to achieve its ends. The last several years have also demonstrated the vulnerability of certain key supply chains—such as semiconductors, critical minerals, and clean energy technology—to these same goals.

Enactment in 2018 of both FIRRMA and the Export Control Reform Act (ECRA) was largely precipitated by this growing threat and the potential risk gaps manifested by foreign actors' activity vis-a-vis U.S. businesses involved with cutting edge technology. Now, as another step to counter the PRC's thirst for advanced technology and to remedy certain supply chain vulnerabilities, both Congress and the Biden administration are considering potentially sweeping authorities creating a new Government agency with new powers to block international business transactions—that is, to oversee American firms' allocation of resources, property, and capital outside the United States.

A version of this new interagency panel was considered in the semiconductor bill earlier this year—a Committee on National Critical Capabilities (CNCC). The CNCC would have limited capital investments, sharing of intellectual property and know-how, financing, and even sales, that could benefit a “country of concern” in a sweeping list of sectors. Many key terms were broad and undefined, and left substantial latitude to the Executive branch to expand the “critical” sectors within its purview and to designate the cabinet secretary accountable for leading it. Virtually every U.S. business, private or public investment fund, and bank engaged in international business could have been impacted if a transaction implicated the “influence” of a country of concern, and could have been compelled to share confidential

deal details and obtain the Government's permission to proceed. Even foreign entities in third countries transacting with, or influenced by, such a country could have been impacted. Subsequent proposals were narrowed, but I believe more homework is still necessary.

Recent media reports say that the Biden administration is close to creating an outbound screening tool by Executive order. To be clear, I hold the strongest view that creating an investment screening mechanism by Executive order would be a significant mistake. Rather, Congress, collaborating with and receiving key input from the Administration, is best suited to assess and respond to an issue of this complexity and potential scope and impact.

There should be no dispute that to ensure America's future security the PRC's theft and misappropriation of technology must be prevented. The question is whether a new committee and bureaucracy of potentially immense scope and authority is the answer. The debate has seemed to take on a life of its own, with an apparent presumption that an outbound screening committee is necessary. The threat from the PRC is real and present, not over-the-horizon, but decisionmakers would benefit greatly by resisting the temptation to rush into a "solution" without adequately assessing the extent to which it will both enhance national security and avoid creating unnecessary burdens on U.S. persons' business transactions.

With this context, I commend the Committee for taking the initiative with today's hearing. There should be more such hearings before any solution is enacted—to define the objectives, determine costs and benefits, and assess whether existing national security authorities could better meet the challenge.

When a bipartisan Congress and the Trump administration worked together to formulate the most extensive changes to CFIUS in its nearly 50-year history, those efforts included roughly a half-dozen hearings with foreign policy and national security experts, the Intelligence Community, private sector stakeholders, and former and current senior Executive branch officials. Congress and the President were thus well informed as to the gaps they intended to fill, where the expanded jurisdiction would reach, and the attendant increases in capacity and cost. The resulting strong, stand-alone bill resoundingly passed. Afterwards, it took 2 intensive years within an existing CFIUS bureaucracy, including at the Cabinet secretary level, to effectively implement the law. Here, an outbound screening mechanism would be created out of whole cloth with, among other things, little to no clarity or consensus yet on who has the capacity and institutional heft to effectively implement the tool and be held accountable.

As with FIRRMA, decisionmakers would be best served by building a comprehensive record-taking testimony from experts and key stakeholders, including senior Administration officials. That effort should explore whether existing or other types of authorities could be less bureaucratic and costly, and more precise and impactful, in achieving the ends—such as adjusting CFIUS's existing jurisdiction, expanding current economic sanctions against Chinese military companies, or modifying export restrictions. These tools do not appear to have been fully considered, but they may in fact offer a better cost/benefit calculus.

Upon first defining the precise risk gap requiring action, and then considering the full spectrum of potential authorities available, a considered and careful assessment of a new outbound investment regime might as an initial matter examine:

- the financial and human resources required;
- the potential U.S. business compliance costs;
- which agency should be accountable for leading implementation and operations;
- precisely which technologies or sectors warrant investment screening, and why;
- the anticipated impacts on the American economy and global capital flows;
- the extraterritorial effects and likely consequent response from allies;
- the extent to which such a mechanism furthers the decoupling of the world's two largest economies—and whether that is a desired policy outcome;
- the extent to which restrictions on U.S. person transactions would be simply replaced by other capital or intellectual property sources; and,
- the extent to which such a tool would have a "national security" standard, as distinguished from a "national interest" standard (that is, whether such screening would be intended for broad industrial policy/strategy).

From my experience in Government and with the interagency process, and particularly in leading CFIUS, I expect that a new committee or screening mechanism would be time- and resource-intensive. It would require substantial energy and effort to build an effective, clear, and precise regulatory framework, and to hire the key human capital and expertise needed to ensure success. The argument that

CFIUS itself could be “leveraged” for this mission also brings the risk of diminishing the capacity of CFIUS to effectively execute its current charge.

It is my privilege to appear before you today and to contribute to your scrutiny of a very important issue consequential both to national security and the U.S. economy. I would be happy to answer any questions that you may have today, and to be a future resource for the Committee.

In sum, to H.L. Mencken is attributed the wisdom that “for every complicated problem there is a solution—easy, simple, and wrong.” In the interests of national security, a strong, open economy, and accountable Government, all Americans should hope and expect that policymakers get this right. The alternative could be an unrestrained bureaucracy, wasted time and resources, and no meaningful response to the PRC’s ominous goals.

PREPARED STATEMENT OF ROBERT STRAYER

EXECUTIVE VICE PRESIDENT OF POLICY, INFORMATION TECHNOLOGY INDUSTRY COUNCIL

SEPTEMBER 29, 2022

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 2 to 5 years. This rapid innovation pace is evidenced by the Moore's Law concept of computing power on a semiconductor doubling every 2 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 6 years.

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 percent 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:

¹Information 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/>.

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 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,

²Testimony 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>.

³See <https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list/ns-cmic-list>.

⁴Securing 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>.

⁵Securing 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>.

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 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

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

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 from 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.

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR SINEMA
FROM SARAH BAUERLE DANZMAN**

Q.1. A few months ago, Congress passed the CHIPS and Science Act, including funding provisions I spearheaded to bolster and expand domestic semiconductor production. How, if at all, do you anticipate this funding might affect a firm's approach when considering outbound investment? Do you believe the level of Federal support is sufficient enough to convert some outbound investment into domestic investment?

A.1. The semiconductor industry is highly subsidized abroad and the CHIPS and Science Act is an important step in allowing U.S. semiconductor firms to operate on a level playing field with companies that receive subsidies in other jurisdictions. I do think that this funding will attract at least a handful of fabrication facilities. Already, we have seen over 20 announcements of new investments in the U.S. in the semiconductor industry over the last 2 years. You can see a list here: <https://semiengineering.com/where-all-the-semiconductor-investments-are-going/>.

The relationship between domestic investment and outbound investment is complex. However, on balance, we should assume that the decision to build a fabrication facility in the U.S. means that the company in question chose not to build in another location. The safeguard provisions in the CHIPS and Science Act similarly will incentivize companies who receive subsidies from investing in advanced semiconductor activity in China.

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR SINEMA
FROM RICHARD ASHOOH**

Q.1. A few months ago, Congress passed the CHIPS and Science Act, including funding provisions I spearheaded to bolster and expand domestic semiconductor production. How, if at all, do you anticipate this funding might affect a firm's approach when considering outbound investment? Do you believe the level of Federal support is sufficient enough to convert some outbound investment into domestic investment?

A.1. Response not received in time for publication.

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR SINEMA
FROM THOMAS FEDDO**

Q.1. A few months ago, Congress passed the CHIPS and Science Act, including funding provisions I spearheaded to bolster and expand domestic semiconductor production. How, if at all, do you anticipate this funding might affect a firm's approach when considering outbound investment? Do you believe the level of Federal support is sufficient enough to convert some outbound investment into domestic investment?

A.1. Response not received in time for publication.

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR SINEMA
FROM ROBERT STRAYER**

Q.1. A few months ago, Congress passed the CHIPS and Science Act, including funding provisions I spearheaded to bolster and expand domestic semiconductor production. How, if at all, do you anticipate this funding might affect a firm's approach when considering outbound investment? Do you believe the level of Federal support is sufficient enough to convert some outbound investment into domestic investment?

A.1. Response not received in time for publication.

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD
STATEMENT SUBMITTED BY THE AFL-CIO

Statement for the Record

Submitted by the AFL-CIO

United States Senate Committee on Banking

Hearing on "Examining Outbound Investment"

Thursday September 29, 2022

The AFL-CIO welcomes the opportunity to provide comments on outbound investment.

The AFL-CIO strongly supports efforts to screen the offshoring of production capabilities and critical supply chains to the People's Republic of China (PRC) and other nations of concern. To that end, we have endorsed the National Critical Capabilities Defense Act (NCCDA), bipartisan, bicameral legislation championed by Senators Casey and Cornyn in this chamber, and introduced by Representatives DeLauro, Pascrell, Spartz and Fitzpatrick in the House of Representatives.

The legislation creates a Committee on National Critical Capabilities (CNCC) to review certain transactions by U.S. businesses to offshore capabilities, technologies and capacity that could result in an unacceptable risk to national and economic security. The bill also authorizes the President to suspend, mitigate, or prohibit transactions that pose an unacceptable risk to our nation's interests.

The review process created by NCCDA would protect US supply chains by screening outbound investment and guarding against offshoring of critical capabilities to adversaries like China and Russia. It is a common-sense approach that recognizes how important our supply chains are to our national, health and economic security. From semiconductors to pharmaceutical ingredients, it would provide a needed review mechanism to advance U.S. production and employment. This approach was recommended as part of the most recent unanimously approved report of the bipartisan U.S.-China Economic & Security Review Commission (USCC)[i].

The NCCDA was also included in the COMPETES package that passed the House of Representatives in early 2022.

Some have argued that the NCCDA is too expansive and efforts to weaken the legislation have been proposed so that it only contains a notification requirement for a very limited class of covered investments. A notification-only requirement would simply tell us what we already know—US corporations are investing in critical industries in China and elsewhere at the expense of US workers and our nation's security. In addition, a notification-only provision may not include public disclosure. Without public disclosure it would provide little, if any, benefit.

The AFL-CIO stands firm in pushing for the review requirement contained in the original legislation that would allow outsourcing investments by covered U.S. businesses to be approved or where they undermine our critical supply chains or security, mitigated or blocked.

In addition, we support the provisions in the legislation that cover a range of sectors, including energy, medical, communications, defense, transportation, aerospace, artificial intelligence, semiconductors, and shipbuilding. Congress should not limit coverage to a few industries, such as AI and semiconductors, as unrestricted offshoring across a wide swathe of defense and security sectors put the U.S. at significant risk.

The Chinese Communist Party's (CCP) policies and programs have been designed to expand their capabilities in critical sectors, all too often at the expense of U.S. power and leadership. We have seen our dependence on Chinese sources of supply expand to unacceptable levels. We cannot afford to continue to play into our adversaries' hands and must have policies like those authorized by NCCDA to ensure that we can meet the needs of our people, ensure the strength of our economy and protect our national security.

The AFL-CIO and the working people we represent are clear—we need to limit businesses from shipping our critical capabilities and jobs to other nations who seek to undermine America's national and economic security.

Opponents of these efforts want to continue their support for multinational corporations that are outsourcing our jobs and critical defense and security capabilities to China.

The passage of the NCCDA would be a bipartisan opportunity for Congress to ensure that supply chains in critical areas won't continue to be offshored to China by companies that have fueled the trade deficit, expanded the Chinese Communist Party's power, and undermined U.S. interests.

We thank you for the opportunity to provide these comments.

**STATEMENT SUBMITTED BY REPRESENTATIVE ROSA L. DELAURO OF
CONNECTICUT AND REPRESENTATIVE BILL PASCRELL, JR., OF NEW
JERSEY**

Congresswoman Rosa L. DeLauro (D-CT-03) and Congressman Bill Pascrell, Jr. (D-NJ-09)
Statement for the Record
United States Senate Committee on Banking, Housing, and Urban Affairs
Hearing on "Examining Outbound Investment"
September 29, 2022

Thank you, Chairman Sherrod Brown (D-OH) and Ranking Member Pat Toomey (R-PA) for holding this important hearing on the issue of examining outbound investment. We wish to thank Senators Bob Casey (D-PA) and John Cornyn (R-TX) for co-leading the Senate version of the National Critical Capabilities Defense Act (NCCDA) and our House co-leads Representatives Victoria Spartz (R-IN-05) and Brian Fitzpatrick (R-PA-01).

In a July hearing before this committee, Chairman Brown, you committed to working with your colleagues to address this issue in a vehicle separate from the CHIPS package, which has now been signed into law.¹ We appreciate this step to honor that commitment by holding this hearing today.

We are House champions of the NCCDA. Our legislation would create a new trade tool that brings a whole-of-government response to review a tailored set of outbound investments in specific sectors. This screening process for outbound investments and the offshoring of critical capacities and supply chains would ensure that the United States can quickly detect and address supply chain vulnerabilities and prevent the offshoring of critical production capacity and intellectual property to our foreign adversaries like the People's Republic of China (PRC) and the Russian Federation.

As you may know, our bill was included as part of the House-passed America COMPETES Act and is under discussion by conferees in the conference committee. The common-sense proposal has strong bipartisan and bicameral support and was recommended as part of the most recent unanimously approved report of the U.S.-China Economic and Security Review Commission.

As champions for American workers, we hope you would agree that we must do more to fix our frayed supply chains and empower our government with the authorities to act to address these problems. We cannot be weak-kneed when it comes to standing up to our adversaries, starting with Xi Jinping and Vladimir Putin. We must take all necessary steps to protect the United States supply chain and our national security from foreign adversaries. While we are encouraged by support from the Biden Administration on this issue and have encouraged executive action, we continue to believe that statutory provisions, like the NCCDA, are essential to safeguard our Nation's critical capabilities, national security, and American workers. We seek your support for our efforts and continued partnership to these ends.

Thank you for your attention to our comments. We look forward to working together with Members of this committee, and bicameral colleagues on both sides of the aisle to enact an outbound investment review mechanism in the 117th Congress.

¹ <https://www.youtube.com/watch?v=RHOHGFfRLxg>

STATEMENT SUBMITTED BY BSA / THE SOFTWARE ALLIANCE

**Statement for the Record by
BSA | The Software Alliance**

In relation to
Senate Committee on Banking, Housing, and Urban Affairs
Full Committee Hearing on “Examining Outbound Investments”

BSA | The Software Alliance welcomes the decision of the Senate Committee on Banking, Housing, and Urban Affairs to hold a hearing on “Examining Outbound Investments” on September 29, 2022. We support many of the perspectives represented at the hearing and the concept of a reasonable notification mechanism that relating to investments associated with sensitive technologies the exportation of which is already controlled under US export control laws. However, we do not support the inclusion in the NDAA of the specific outbound investment screening framework envisioned by the National Critical Capabilities Defense Act (NCCDA).

Prior NCCDA proposals that broadly restrict activities across numerous undefined industry sectors could imperil US technology leadership by making it harder for US companies to maintain visibility and access to overseas technology that can be purchased or licensed to make US business and manufacturing operations more competitive. Because foreign competitors from the EU, Japan, Korea, and elsewhere would face no similar restraints, American companies would face a competitive disadvantage.

Prior NCCDA proposals have covered a much wider array of commercial activities than the type of equity or other investments than are currently addressed by the Committee on Foreign Investment in the United States (CFIUS). Furthermore, these legislative proposals have been overbroad in scope and industry coverage, capturing many sectors and technologies that are already commercially available around the world. For example, one recent NCCDA proposal would encompass broad and undefined categories of “artificial intelligence” (AI) or “quantum computing,” which extend well beyond the specific types of AI or quantum technologies for which an export control license would be required.

Finally, we echo several views expressed at the hearing, including that: (a) certain tools already exist under US sanctions and related legal authorities to address national security risks associated with outbound investments; (b) given the significant uncertainty that pervades the issue, Congress should define with precision the specific concerns that it seeks to address in any outbound investment notification mechanism; (c) Congress should duly consider and account for ongoing efforts by the Executive Branch to deal with outbound investments that implicate national security concerns; and (d) Congress should resist the temptation to use outbound investment screening for purposes other than national security;

We urge Congress to act with due care in evaluating outbound investment notification options. Furthermore, any notification mechanism should be scoped to focus strictly on actual investments in countries of concern relating to sensitive technologies the exportation of which is already controlled under US export control laws. Lastly, any such proposal should proceed through regular order, including relevant committee review and hearings. For these reasons, BSA asks you to oppose the inclusion in the NDAA of the overbroad “outbound investment screening” NCCDA discussion drafts that have been publicly evaluated to date.