

NATIONAL SECURITY CHALLENGES: OUTPACING CHINA IN EMERGING TECHNOLOGY

HEARING

BEFORE THE

COMMITTEE ON

BANKING, HOUSING, AND URBAN AFFAIRS

UNITED STATES SENATE

ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

ON

EXAMINING NATIONAL SECURITY CHALLENGES REGARDING CHINA
AND EMERGING TECHNOLOGY

JANUARY 18, 2024

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



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

U.S. GOVERNMENT PUBLISHING OFFICE

60-365 PDF

WASHINGTON : 2026

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

SHERROD BROWN, Ohio, *Chair*

JACK REED, Rhode Island	TIM SCOTT, South Carolina
ROBERT MENENDEZ, New Jersey	MIKE CRAPO, Idaho
JON TESTER, Montana	MIKE ROUNDS, South Dakota
MARK R. WARNER, Virginia	THOM TILLIS, North Carolina
ELIZABETH WARREN, Massachusetts	JOHN KENNEDY, Louisiana
CHRIS VAN HOLLEN, Maryland	BILL HAGERTY, Tennessee
CATHERINE CORTEZ MASTO, Nevada	CYNTHIA M. LUMMIS, Wyoming
TINA SMITH, Minnesota	J.D. VANCE, Ohio
RAPHAEL G. WARNOCK, Georgia	KATIE BOYD BRITT, Alabama
JOHN FETTERMAN, Pennsylvania	KEVIN CRAMER, North Dakota
LAPHONZA R. BUTLER, California	STEVE DAINES, Montana

LAURA SWANSON, *Staff Director*

LILA NIEVES-LEE, *Republican Staff Director*

ELISHA TUKU, *Chief Counsel*

AMBER BECK, *Republican Chief Counsel*

CAMERON RICKER, *Chief Clerk*

SHELVIN SIMMONS, *IT Director*

PAT LALLY, *Assistant Clerk*

C O N T E N T S

THURSDAY, JANUARY 18, 2024

	Page
Opening statement of Chair Brown	1
Prepared statement	42
Opening statements, comments, or prepared statements of:	
Senator Scott	3
Prepared statement	43

WITNESSES

Emily Kilcrease, Senior Fellow and Director of the Energy, Economics, and Security Program, Center for a New American Security	5
Prepared statement	45
Responses to written questions of:	
Chair Brown	96
Senator Cortez Masto	98
Senator Van Hollen	100
Senator Warnock	102
Jamil N. Jaffer, Founder and Executive Director, National Security Institute and NSI Cyber and Tech Center, Antonin Scalia Law School at George Mason University	6
Prepared statement	67
Responses to written questions of:	
Chair Brown	105
Senator Cortez Masto	106
Lindsay Gorman, Senior Fellow for Emerging Technologies, The Alliance for Securing Democracy at the German Marshall Fund of the United States	8
Prepared statement	85
Responses to written questions of:	
Senator Cortez Masto	108
Senator Van Hollen	108
Senator Warnock	108

NATIONAL SECURITY CHALLENGES: OUT-PACING CHINA IN EMERGING TECHNOLOGY

THURSDAY, JANUARY 18, 2024

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

The Committee met at 10 a.m., in room SD-538, Dirksen Senate Office Building, Hon. Sherrod Brown, Chair of the Committee, presiding.

OPENING STATEMENT OF CHAIR SHERROD BROWN

Chair BROWN. The Committee will come to order.

Last week, the Committee heard about the human toll that illicit fentanyl takes on our families, our friends, our neighbors. Witnesses stressed the need to come together to take action to stop the flow of illicit fentanyl from China and Mexico. This Committee, the entire Senate, did—just did that—did just that last year when Senator Scott's and my bill included the FEND Off Fentanyl Act. We were successful together in making it a part of the annual defense authorization bill. It has not been—become law yet, even though it passed the Senate—the bill with our amendment in it passed the Senate, I believe, with 90 or 91 votes—because politicians in the House—extremists in the House have played politics and kept it out of the NDAA.

The FEND Off Fentanyl Act was not the only Committee priority that the House blocked last year. They blocked two other important national security amendments in the NDAA, both of which received more than 90 votes in the Senate. Ninety-one senators voted in favor of an amendment offered by our colleagues, Senator Tester—thank you—and Senator Rounds, whom I saw earlier this morning, to prevent big investors in China from buying up American farmland and food businesses, clearly in our national security interest. We cannot allow foreign adversaries to buy up farmland in Ohio and around the country. It is a threat to our national security. It is a threat to rural economies and our way of life. Ninety-one senators also voted in favor of an amendment offered by Senators Casey and Cornyn, bipartisan amendment to allow us to better monitor U.S. companies' investments that fund Chinese—fund Chinese development of critical technology, including military technology.

All three of these provisions have broad support, from Heritage Action to the Coalition for a Prosperous America. More importantly, they have the support—overwhelming support of the public. For far too long, our policy around China catered to multinational

corporations and do not think the House and Senate were not part of that. They failed State—they failed—that policy failed States like Ohio. In this Committee, we worked to change that. We found common ground. It is why all three of these bills remain top priorities in this Committee. I am committed to working with colleagues to make these provisions law.

Of course, the threats posed by China are many and varied and growing. Our work to address national security risk posed by the Chinese Government should not end with those three provisions. We agree that China poses a real and growing threat to our national security. Perhaps nowhere is that risk more acute than with the development of advanced technology. China has used advanced technology, much of it stolen from the U.S., some of it sent there through corporate outsourcing, to ramp up its military modernization and build a mass surveillance State that commits deplorable human rights violations, including the detention of millions of Uyghurs and Xinjiang.

Addressing these threats from the Chinese Government and improving our domestic capability to compete with China has been a top priority of this Committee. Five years ago, we updated the laws that govern our export control and inbound investment screening programs. Now we must assess whether our current authorities and the resources we commit to them match the threat we face. Export controls can be used to deny China and others access to U.S. technology that they could use to undermine our national security. We have made export controls a central feature of our national security and our foreign policy.

In addition to assembling a global export control coalition in response to Russia's war against Ukraine, the Administration has added hundreds of China-based entities to the restricted trade list and imposed countrywide controls that restrict China's access to advanced semiconductors and tools and equipment needed to produce them. It ramped up enforcement efforts to safeguard our most sensitive technologies, but as Commerce Secretary Raimondo noted, the export control budget of the Bureau of Industry and Security is roughly the same as it was a decade ago, despite its ever-increasing workload.

If we agree that export controls are critical to our national security, and I think we all do, then that is not good enough. We need a China policy for the world we live in today. We must prepare for what could come tomorrow. It means we must upgrade our economic security authorities and resources, accelerate efforts to persuade other countries to join us, and enhance our analytical capabilities so that we can better understand the effects that our economic security tools have on China, on U.S. companies, on companies and partner countries.

Well, today—we will discuss today with our three witnesses how we should rethink and reorient how economic security programs are implemented to address the full range of risks posed by China. We will examine how we can strengthen these authorities and resources to build a stronger, more responsive economic security policy. Our country's policies regarding China have failed for too long. And they have been written, and, historically, we know this—they have been written, aided, and abetted by the Senate and the House

and Presidents of both parties who sold out American workers, pure and simple, to increase the profits of multinational corporations, always, always, always looking for cheap labor, not to benefit national security, not to benefit American workers. This is on—this is on everyone that participated in this.

We know that when companies outsource jobs, they outsource innovation. They outsource technological capabilities along with it. We live with the consequences. Look at the solar industry. Look at semiconductors. We cannot allow China to continue to use that technology. In many cases—say it—they stole it to enhance its military capabilities. We can agree that China is a real growing threat. Countering that threat and updating the failed policies of the past will continue to be a bipartisan focus of this Committee. I thank Senator Scott for that, and I know it will continue. Yeah.

OPENING STATEMENT OF SENATOR TIM SCOTT

Senator SCOTT. Thank you, Mr. Chairman. Good morning to the witnesses. Thank you for being here as well. Thank you, Mr. Chairman, for this opportunity to talk about such an important topic, but before turning to this hearing, I would like to take a moment and draw attention to the recent Iran-backed strikes in Iraq.

Anytime American lives are put at risk, whether it is from Iran or their terror proxies like Hamas, we need to have a strong response, and that starts with this chamber passing my Revoke Iranian Funding Act. Every dollar that goes to Iran from this Administration's actions is a dollar that supports terror. Thank you.

America is the land of opportunity and freedom, the opportunity to innovate, produce, and execute on individual ideas. These principles are what drives our strides in technological innovation and our emphasis on entrepreneurship. We have the strongest economy in the world, driven by its dynamic growth and evolution. We are the global gold standard that countries look on with envy. However, American exceptionalism is under attack from a country that does not want to play by the rules. That country is obviously China. To make sure our success does not become the victory of others, the U.S. Government must act strategically and with strength in protecting opportunities for growth at home and abroad.

When we look at adversaries like the Chinese Communist Party, with their centrally planned economy that actively works to distort global markets for its own gain and continuously makes overt attempts to oust U.S. from our perch of leadership, we do not have to ask the question are they playing by the rules because we already know the answer to the question, and the answer is emphatically no. But China's approach, with their controlled markets, Government interventions, and intellectual property theft, is shackled to the openness of others, so we must act strategically to ensure that we are safeguarding America's treasure: our ability to innovate. We cannot let China continue its malign activities, especially in regards to using or even stealing American innovation and American technologies for nefarious purposes, like advancing its rapidly growing military.

So as we consider American security and prosperity from the Banking Committee's jurisdiction, we should look first at our eco-

conomic security tools. We need to examine the authorities provided to the executive branch, how they have been used, and how they can be improved for maximum effectiveness. However, an over application of these tools has the potential to push our adversaries closer together and damage the U.S.' and our industry's long-term abilities to innovate and generate jobs and to generate growth. Therefore, our use of these tools must be sharp but tailored.

Thankfully, we can isolate bad actors through our sanctions policies, we can restrict malign investment through our CFIUS process, and we can curtail the export of critical goods and services to our enemies. These actions are stronger when we work together with our allies and stay focused on the true problem at hand, but, unfortunately, this Administration has yet again taken the wrong approach. This Administration has put politics over policy and in some ways, that is playing right into the hands of China.

For example, the Department of Commerce's Bureau of Industry and Security, the steward of our export controls, is currently engaging in politically motivated attacks against the illegal firearms industry, a troubling trend. This Administration's regulators try to target lawful businesses through the regulatory process that do not fit their political narrative. This undercuts the Commerce Department's important mission of safeguarding U.S. technology, opening the door for distractions that will allow the CCP to take advantage.

But the Commerce is not the only perpetrator. The Department of Treasury's primary focus appears to be on pursuing the limits of climate and green energy financing policy, and frankly, these objectives only advance China's solar and critical mineral energy positions in geopolitical affairs. Treasury's time, attention, and taxpayer-provided resources will be a much better spent working to ensure our sanctions policies on China remain up to date and promoting as well as protecting American industry abroad. We need an Administration that is focused on countering the real threat—China—not one that is more interesting to politics.

So while I am grateful that we have such an esteemed panel before U.S. today, I think it is imperative that we hear directly from the Administration as well. That said, I look forward to hearing from each of you and your expertise on the issues that will help strengthen our economy and strengthen our position against China and, importantly, to learning more from their perspectives on how we should act and respond to the threat.

Chair BROWN. Thank you, Senator Scott. Emily Kilcrease is a senior fellow and direct—the director of the Energy, Economics, and Security program at the Center for a New American Security. Ms. Kilcrease, thank you for joining us. Jamil Jaffer is the founder and executive director of the National Security Institute and assistant professor of law at George Mason University. Welcome. Lindsay Gorman is senior fellow for emerging Technologies at the German Marshall Fund's Alliance for Security—Securing Democracy. Welcome, Ms. Gorman. Thank you all for being here. Ms. Kilcrease, please begin.

STATEMENT OF EMILY KILCREASE, SENIOR FELLOW AND DIRECTOR OF THE ENERGY, ECONOMICS, AND SECURITY PROGRAM, CENTER FOR A NEW AMERICAN SECURITY

Ms. KILCREASE. Good morning. Chairman Brown, Ranking Member Scott, Members of the Committee, it is an honor to be here speaking with you today. My comments draw from a large body of research that I have conducted on economic security issues at the Center for a New American Security, as well as my prior experience proudly serving in economic security roles in the U.S. Government, and please let me note, I am speaking today in my personal capacity.

As Secretary of State Anthony Blinken has stated, China is the only country with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to do it. The China challenge presents unique difficulties compared to prior eras of strategic competition given China's deep integration with the U.S. and global economies, which creates new types of national security risks arising from economic entanglement.

Russia's brutal invasion of Ukraine and the increasingly authoritarian bent of China under Xi Jinping means that U.S. policy cannot rely on the deterrent effect of economic ties. It must instead focus on mitigating the national security risks arising from the economic relationship, prevent China from exploiting the open nature of the U.S. market, and anticipate future risks that may emerge due to the rapid global advance of critical technologies. These are formidable challenges and will require the Government to prioritize economic security programs, and as Congress considers ways to strengthen the capacity of U.S. economic security programs, key themes emerge across all of the programs related to strategy, evaluation, resources, and international partnerships.

On strategy, the United States needs, but does not have, an economic security strategy, one that is integrated with our national security strategy and provides clear direction on how the United States will use all of its tools of economic statecraft in tandem to protect its economic and security interests with respect to China. A clear strategy will also facilitate conversations in alignment with key international partners. On evaluation, the United States is using economic security tools in greater and more clever ways than ever before, yet it does not have robust processes to assess whether these tools are actually working. It should, and it should include a clear-eyed look at the impact of these tools on U.S. competitiveness and U.S. alliances.

On resources, implementing and enforcing a greater scope of economic security programs will require resources, and importantly, this means not just more money, but more money well spent, prioritizing those investments that can add efficiency and analytic rigor to the economic security programs. On international partnerships, a unilateral approach to economic security will not be a durable one as foreign firms rush to backfill U.S. technology exports and investments in China. China fears a united West, and it is critical that the United States leverage its advantage of alliances as it manages the strategic relationship with China.

In addition to these cross-cutting themes, let me share brief thoughts on the set of economic security tools that we will be talking about today, and I will start with export controls. The United States is implementing new and more innovative types of export controls, including countrywide controls on commercial technologies in response to China's military civil fusion strategy and novel extraterritorial controls, including the foreign direct product rule.

As export controls play a more central role in U.S. foreign policy, the capacity to enforce these rules while also evaluating their effectiveness, and, on top of that, assessing the need for additional controls, remains a bureaucratic challenge. Implementing new controls in emerging tech areas is particularly difficult as technology moves faster than Government can adopt policies in response. The budget for export controls has remained flat in real terms for over a decade. Additional resourcing, which Commerce Secretary Raimondo has called for, can enable much-needed investments, including related to export enforcement, regular review and updating of the Control List, and longer-term efforts to strengthen cooperation with international partners.

Turning to CFIUS, first, I commend Congress for its keen focus on resources as part of the 2018 FIRRMA updates to the CFIUS process. This focus and attention has enabled CFIUS to effectively implement its expanded FIRRMA mandate. As Congress considers further updates, I encourage you to consider expanding the CFIUS definition of critical technologies to allow CFIUS a stronger ability to review transactions involving emerging tech areas, and CFIUS—oh, excuse me—Congress can also reduce mission creep by CFIUS by passing data security and data privacy legislation, issues that consume significant CFIUS resources simply because there are no other authorities to deal with those concerns.

Finally, on outbound investment, Congress should establish new authorities to regulate U.S. investments in China. An outbound investment program should focus on those specific transactions that may convey nontechnical industrial know-how to China in critical technology sectors with relevance to U.S. national security interests. An effective design will include mandatory notifications, targeted prohibitions of investments in technologies that represent high national security risk, entity-based restrictions for particular bad actors, and end-use restrictions.

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

Chair BROWN. Thank you, Ms. Kilcrease. Mr. Jaffer, welcome.

STATEMENT OF JAMIL N. JAFFER, FOUNDER AND EXECUTIVE DIRECTOR, NATIONAL SECURITY INSTITUTE AND NSI CYBER AND TECH CENTER, ANTONIN SCALIA LAW SCHOOL AT GEORGE MASON UNIVERSITY

Mr. JAFFER. Thank you, Chairman Brown, Ranking Member Scott, and Members of the Committee. I appreciate the opportunity to be here to talk about the very real threat, the very real national security threat that China poses to our country and the connection between that threat and our ability to innovate and emerging technologies here in this country. I want to thank the Chairman and the Ranking Member for their leadership on issues related to

China, including your leadership on the critical issue of fentanyl crossing our Southern border from China that is killing thousands of Americans on a yearly basis.

When it comes to China and emerging technology, the facts are this: China has built its economy on stealing American and allied intellectual property. Millions and billions of dollars in total of American research and development dollars walk out the back door to China every year. That research development money is critically important to our ability to ultimately succeed in the larger economic, political, and military conflict with China. We will not win on steel. We will not win on population. We will only win if we out innovate China and outwork China.

We can and will and have done this in the past, and we can and will do it again, but it requires significant action. It requires preventing American companies from transferring significant amounts of American technology to China inadvertently, whether through theft, forced IP transfers, joint ventures, or the like. The Chinese know how to manipulate our desired access to their markets in order to get our intellectual property. They have done it before. They will do it again. We need to work tightly with industry to ensure that does not happen.

At the same time, we need to build capability in this country. That means providing the kind of tax and economic incentives to our companies to build and innovate here and to keep that intellectual property here in this country. It also means doing no harm. It means avoiding overregulation. It means avoiding selective enforcement of existing laws or modifying existing law to target our key innovative—most innovative companies in this country. Seventy percent of research development dollars in this country are spent by the private sector. Seven of the top 10 R&D spenders in this country are technology companies, including every single one of the top five. Going after our technology companies in an environment of competition with China makes little to no sense.

At the same time, we need to ensure that we are incentivizing Americans, American companies, American entrepreneurs and investors to invest here. That means ensuring that we have the right structures and regulatory procedures in place to ensure that investments are free, open, and fair. That also means that we need to work with our investors to ensure that they do the right thing as well. There is no good reason why American investors should be investing in our adversaries' technology. They should be investing in American technology. We can incentivize that, and they have a benefit, too.

Our capital allocators in this economy benefit from living in a free and open society. They benefit from an economic tax system that is the one that this country built. As a result, they should already be incentivized to voluntarily work to invest in American technology, American defense technology, and not in that of the Chinese, the Russians, the Iranians, or the North Koreans.

Ranking Member Scott mentioned what is going on today in the Red Sea with the Houthis. He mentioned the ongoing attacks by Iran against Americans in Iraq and Syria. We must realize that the war in Ukraine, the potential threats against Taiwan, and Iran's bad behavior in the Middle East are not unconnected. China is

working directly with Russia on its war in Ukraine. It is working directly with Iran on the provision of missile technology. It is working with North Korea on its nuclear program. China is at the heart of all of this. As a result, it is imperative that in this country we work tightly, hand in glove, industry with Government, bringing the right incentives, the right opportunities, preventing overregulation, ensuring that we work collaboratively to move this country forward.

One last note. It is critical that we build a STEM-capable workforce in this country. That means investing in education and basic science research. It also means fundamentally fixing our broken immigration system. The idea that we bring thousands of foreigners to this country every year, the most brilliant in the world, to be educated and receive Ph.D.s in our universities and then force them to return home to build their companies and invest abroad is ridiculous. The idea that we have a system based on a lottery is crazy. We should pick the best and the brightest in the world and incentivize them to stay here and become part of the American Dream. That is what America always has been. It is what we should be in the future. It is how we will ultimately beat China economically, militarily, and politically.

Thank you for the opportunity to be here today. I look forward to your questions.

Chair BROWN. Thank you, Mr. Jaffer. Ms. Gorman, welcome.

STATEMENT OF LINDSAY GORMAN, SENIOR FELLOW FOR EMERGING TECHNOLOGIES, THE ALLIANCE FOR SECURING DEMOCRACY AT THE GERMAN MARSHALL FUND OF THE UNITED STATES

Ms. GORMAN. Chairman Brown, Ranking Member Scott, and Members of the Committee, thank you for the opportunity to testify before you today. I come at this issue as a researcher leading a team focused on technology and geopolitics at the German Marshall Fund, as a former policy professional developing allied technology cooperation initiatives, and, in a past life, as a scientist in the lab conducting quantum physics experiments and building artificial intelligence systems. I speak here today in my personal capacity.

The United States has spent decades investing in, inventing, and reinventing new modes of warfare, modernizing our military in response to new adversary capabilities and threats. In the 1950s, the Pentagon's first offset strategy emphasized building up the U.S. nuclear arsenal to offset perceived conventional force disadvantages vis-a-vis the Soviet Union. When the U.S.S.R. gained nuclear parity in the late 1970s and early 80s, the second offset strategy bet on precision strike and stealth technologies. Recently, a third offset strategy sought to reestablish flagging U.S. military technological superiority.

Today, the United States' strongest autocratic rival uses tactics in economic, technological, and societal realms that a defense-first national security apparatus was not designed to counter. In the PRC, we face a competitor who wields its own economic power to coerce Nations, businesses, and individuals to achieve its technology and national security objectives. This multisectoral competition has strained the post-cold war view of international relations,

in which more economic engagement has implied greater political, even democratic proximity.

Much as we have in the past, the United States today must reorient and invest in new capabilities and tools to meet this threat. A key element of this effort is building out a doctrine, toolkit, and alliances for techno-economic statecraft. Some of these tools already exist, but many were designed for a different era, when their remit was far simpler in terms of ensuring that technology items with dual-use capability—those that could be used for both military and particular weapons of mass destruction, and civilian uses—were used for the latter and not the former in countries of concern.

These dual-use applications often had clear signatures—uranium enrichment thresholds, for example—signifying use for civilian nuclear power or as weapons-grade nuclear fuel. These modes are outdated and unfit for our modern challenges for three reasons.

First, straightforward distinctions and thresholds between military and civilian applications of emerging technologies rarely exist. The same quantum computer that could revolutionize scientific discovery could break the encryption that secures our communications with submarines. The same synthetic biology processes that could engineer novel cancer therapies could also engineer pandemic pathogens, and the same computing capacity that fuels large language models can fuel drone swarms and mass surveillance. Second, the PRC's strategy of civil-military fusion further blurs these lines, making it difficult to have any confidence that any civilian use will stay a civilian use. And third, many of today's national security technology risks simply fall outside the military domain, such as human rights abuses, the promotion of autocratic values and standards in emerging technologies, and strategic dependencies in critical supply chains.

Outpacing China no longer simply means outrunning the PRC but also impeding its capabilities in key force multiplier technologies. This will require the United States and its allies to control capabilities, not only technologies. In my written testimony, I discuss the inputs and considerations for controls in AI, biotechnology, and quantum information and provide recommendations along three lines. First, significantly expand U.S. and allied analytical capacity, including by establishing a national technology competitiveness analysis center; second, leverage cutting-edge technologies to track and control—to track control evaluations and evasions and bolster enforcement, from knowledge graphs and link chart analyses to data bases of Chinese entities and partnerships; and third, build capacity among U.S. allies and partners on novel techno-economic statecraft tools and approaches modeled off FIRRMA's CFIUS expansion.

Thank you, and I look forward to your questions.

Chair BROWN. Thank you, Ms. Gorman. I will start with just an observation before I turn to Ms. Kilcrease for a question. Mr. Jaffer said that, essentially, that we need to incent U.S. corporations not to invest in China. These are the same corporations that lobbied this Congress 25 and 30 years ago, very successfully, because many of my colleagues like to be at the beck and call of corporate interests, because labor was too expensive in the United States, even

too expensive in the Southern—the non-union South, and lobbied for first most favored Nation status.

They decided that did not sound very good, so then permanent normal trade relations with China. U.S. corporations moved jobs overseas, benefited from it. Their bottom line: their stockholders benefited. American workers in my State, especially in my part of the country, were left behind. Now those same companies, we need to incent them not to invest in China. I mean, I do not disagree with that, but it is really a pretty remarkable irony of history. I will stop there.

Question for Ms. Kilcrease and Ms. Gorman: Secretary Raimondo recently said the export control budget at BIS is roughly the same as it was a decade ago—you each mentioned that—from responding to China's—with an increasing workload, responding to Russia's invasion of Ukraine to new countrywide controls and chip exports. Both of you, quickly, if you can, two questions. Can you each describe what resources—technology, information, personnel—Congress should provide to BIS to meet its growing export control mission? What are the negative implications of not increasing funding? Start with you, Ms. Kilcrease, and you, Ms. Gorman.

Ms. KILCREASE. Thank you for the question. It is an incredibly important one, and I will quickly go through what could be a long laundry list on that. But there is a range of needs in the Department of Commerce as well as the other export control agencies. It is not just Commerce that has responsibility for implementing these. The bread-and-butter functions of license applications and export control enforcement absolutely need additional funding, but one thing I talk a lot about in my written statement is that we need to be spending these new resources wisely. We need to be really investing in the evaluation and analytic capabilities so that the Department of Commerce is not just relying on industry input but has access to a wide range of unbiased information as it is building up its capacity to evaluate and assess whether controls are actually working in practice. We do not have that capacity. We need that capacity, and it needs to be an unbiased kind of independent analytic capability.

We need to invest in the international engagement function so we are not implementing controls unilaterally and we can really put in the political elbow grease to make sure we get partners and allies on board, and we need to be examining new ways of doing technical export control enforcement. I will flag some work that my colleague, Tim Fist, has done looking at, for example, on chip governance. It is a way to do smarter enforcement, not just more enforcement.

I fear if we do not make these sorts of investments, the export control system will continue to be outdated. It will continue to be stuck in a kind of a cold war mentality, and it will continue to fail to capture the emerging technologies that are really at the center of the U.S. China competition.

Chair BROWN. Thank you. Ms. Gorman.

Ms. GORMAN. Yes, I very much agree with Ms. Kilcrease's response and would add that on the analytical capacity, part of what we are talking about is we do not have the tools to understand the downstream economic impacts to United States businesses and to

China's own capacity development if we restrict certain critical technologies today. We need to make—be making these decisions based on red team/blue team analyses, forecasting projects 5, 10, 20 years into the future, so that it is not about just slapping a control on one tiny bit of technology but really trying to limit the capabilities of China into the future, and we are making smart investments in those controls.

This is what this kind of analytical center should do. We should not be leaving it to companies, even to researchers, to Members of Congress. We need the best information available. That also includes robust data bases that can draw information from all sources—from Chinese financial sources, that can track when Chinese entities pop up that are subsidiaries. They have a strategy now. Once they get put on an Export Control List, we see five new companies of a similar name popping up doing similar things. We need to be better at automatically adding those entities into our Control List and creating data bases and leveraging tools, like AI and data science, to be tracking those networks of smuggling sanctions evasion and these creative ways that China can circumvent our export controls. And then last, on the multilateral cooperative—

Chair BROWN. Quickly.

Ms. GORMAN. Yes.

Chair BROWN. Got it. OK. All right. Thank you. The other question I want for you, Ms. Kilcrease, I wanted to ask you about the Casey-Cornyn issue of outbound investment. Describe the regulatory gap that outbound investment authority would fill, and, if you can, as quickly as possible, why is it important for Congress to enact outbound investment legislation if an Executive order already exists?

Ms. KILCREASE. Yeah. So I do think that there is a growing body of evidence that certain U.S. investments in China do present national security risks, and there is a gap in the authorities to address these. You know, the most common tool that people will raise is that of export controls, which regulates the transfer of technologies to China and other destinations, but the problem is that only captures part of the risk. It does not capture nontechnical information or industrial know-how that is nonetheless critical for advancing a country's capability in a particular technology ecosystem.

The example that I think is most helpful is to think about a semiconductor fab, where when you think about what it takes to churn out chips at scale efficiently and on cost-competitive terms, that requires complex supply chain management. It requires a skilled workforce, the recruiting and retention of that sort of skilled workforce. It includes commercial strategies that can survive in a cutthroat environment. None of that is suitable to be captured under export controls, but it is, again, nonetheless critical for how China will build its capacity. And it is this exact sort of know-how that flows along with an investment, and we do not have a tool to capture that currently.

So clearly, there has been a lot of debate on this, including in Congress and in the Administration. Substantively, I think the Administration's Executive order is headed in the right direction, but,

ultimately, it is far better for these sorts of programs to be codified by Congress, particularly because we have this great example in the FIRRMA process where Congress was really able to shape and guide and provide appropriate resources to provide a clear legal mandate for what they wanted the executive branch to do. So ultimately, I do think it is incumbent on Congress to act on this problem.

Chair BROWN. Senator Scott.

Senator SCOTT. Thank you, Mr. Chairman, for my 10 minutes, and I will start today.

Chair BROWN. Five plus 2 equals 7.

Senator SCOTT. Well, in Washington math, that is 10.

Chair BROWN. Oh. Do you write his jokes?

Senator SCOTT. He agrees with my jokes. Thank you, Senator Tester. He is eating in way at my time, by the way, as well, so 11 minutes.

Chair BROWN. —before you—

Senator SCOTT. Thank you, sir.

Chair BROWN. —10 and it is 11.

[Laughter.]

Senator SCOTT. OK. Sorry about that. One of the largest pillars in China's campaign of economic coercion is this systematic theft of our IP. We have seen it time and again, from the corporate world to computing to agriculture, and what I find deeply concerning is that we are now seeing it on our college campuses, university campuses. I have written several letters to the Biden administration on this subject, and, thankfully, my amendment on gifts and grants from Chinese military firms to our institutions of higher education was signed into law in the last year's NDAA. Thankfully, with this report now, the Departments of Treasury and Education will be required to provide a full accounting of the donations that the Chinese military firms are providing to U.S. educational institutions, an important first step in the right direction.

Mr. Jaffer, you are an academic. You are on college campuses. Talk to me a little bit about the national security threat that China's influence presents on our college campuses.

Mr. JAFFER. Thank you, Ranking Member Scott. The idea that we would allow Chinese influence operations to take place on our college campuses through Confucius institutes, through research collaborations and the like, is deeply concerning. We know that the Chinese Government is engaged in a concerted effort to steal intellectual property, not just through cyber means, although that is the predominant means by which they do it, not just through physical capabilities by putting people in American companies and stealing that innovation, but by stealing core R&D taking place, basic science research in our colleges and universities, and they are doing that through these research collaborations.

Now, there are collaborations that make sense with allied Nations. There are collaborations across borders that make tons of sense, but collaborating with Chinese researchers who we know are influenced and pressured by the Chinese Government on a regular basis to steal intellectual property simply makes no sense. Taking cash money from Chinese companies who have ulterior motives simply makes no sense. No university should do it, and I applaud

you, Senator Scott, for having outted this fact and for calling it out once and again.

Senator SCOTT. How do we—if you—if you were in charge, how would you help U.S. stop or reduce the amount of activity on those college campuses? How much further can we go than just the amendment that was a part of the NDAA in spotting it, bringing light to it? In addition to that, we have 300,000 or so Chinese students on our college campuses. I am not sure how many report back to the CCP, but it is a concern to me. I would love to hear your thoughts on that as well.

Mr. JAFFER. Well, look, we always have to be careful to not, you know, tar every Chinese student that is here in the United States with the brush that they are working with the Chinese Government, but we have to recognize the Chinese Government is engaged in an active effort to bring students here, to bring researchers here, to work with American academics here in this country, pay them to transfer technology. The Thousand Talents Program and the like are a few examples of those.

Now, in order to ensure that this does not happen when we bring students in, bring Chinese nationals in, vetting them—frankly, nationals from any country—vetting them well, ensuring they are not a national security risk is an important part of that immigration process, including for students and the like and researchers. At the same time, Federal—universities obtain a tremendous amount of Federal grant money. They obtain a tremendous amount of Federal financial aid for their students. Making those pipelines hard to access if they continue to allow their research and development to walk out the backdoor to China is a very significant penalty you can leverage. Now, I am not saying we should do that. I am saying we need to think cautiously about that.

At the same time, if our universities are allowing this to happen and they know it is happening and are not taking action to stop it, public and private alike, action can be taken to make their lives a lot more difficult.

Senator SCOTT. It sounds like a carrot-and-stick approach, though. You put ourselves—you put the Nation and the universities in a strong position to speak clearly and make good decisions with consequences. Without those consequences, to me, it seems like there will be—we cannot reinforce good behavior if all we are saying is “please.”

Mr. JAFFER. That is exactly right, and, you know, it goes to universities, it goes to investors alike. All of us have an incentive to do the right thing, right, to invest in American technology, protect our intellectual property, and ensure innovation stays here, right? We should recognize that because we live in this system of governance, in this economic system, benefiting our adversaries is actually contrary to all of our interests, and as a result, universities already have the incentive to do the right thing. Investors have the incentive to do the right thing. Providing them more incentives, and ultimately only reaching for the regulatory stick when you absolutely have to is ultimately, I think, the right approach.

Senator SCOTT. Thank you.

Chair BROWN. Thank you, Senator Scott. Senator Menendez of New Jersey is recognized.

Senator MENENDEZ. Thank you, Mr. Chairman. Last Congress, I introduced the Economic Statecraft for the Twenty-First Century Act, a bill that provides a comprehensive plan to confront the anti-competitive, predatory nature of China's international economic policies. The legislation would allow U.S. to lead to our values by strengthening our supply chains with reshoring, nearshoring strategies, by achieving our energy-related sustainability goals, by fostering cooperation in multilateral institutions, by building global resiliency, among other things. So my question, Ms. Kilcrease, what effective economic tools do we presently have to have the United States be able to deal with our China challenge, and what, if any, additional authorities do you believe would be beneficial for U.S. in terms of leading our economic diplomacy?

Ms. KILCREASE. Thank you for the question and for your leadership in developing economic statecraft strategy. It is critically important that as we think about the specific tools, we are also thinking about how all of these tools work in tandem to achieve our goals, and particularly if we are talking about technology leadership, and leadership in particular sectors, assessing these tools and how they work together is so important.

You know, I think we have a growing body of tools that are effective. Some of our export controls, our investment screening, these are mature processes where there is always room for improvement, but we have well-established frameworks. We also have robust industrial policy at this point in the U.S., where we are really trying to implement the run faster part of the agenda, trying to invest in our R&D capabilities and strengthen our STEM capabilities as well. Ultimately, these are all the sorts of efforts that need to move forward in tandem.

But that does not mean that our work is done, of course, right? We are talking today about outbound investment as one of the key ways to protect our economic security interests. We should also be having a conversation around tariff restructuring and how that could potentially be used in some cases to protect against Chinese unfair trade practices. That requires deep analysis, economic analysis of downstream impacts, but it is one of the areas where we do have a gap, and we need to consider, again, whether that sort of approach would advance our interests.

Senator MENENDEZ. Thank you. I want to talk about our lack of outbound investment oversight in sensitive industries that has the potential to harm our national security and hamper the competitiveness of U.S. industry because of the technical prowess, capital, and the unique know-how that access to the U.S. capital markets provide. President Biden's Executive order in August is a good start, but I fear it may be too limited. Ms. Gorman, is the order broad enough to prevent U.S. capital and expertise from financing the wide range of critical sectors that undermine U.S. national security?

Ms. GORMAN. Thank you for the question. I think the order itself, which focuses on AI, semiconductors, and quantum information systems exclusively, I think, can be seen, as you rightly point out, as a good start. We may in the future want to look at similar outbound investments on other critical and emerging technology areas, but this depends on where we have strategic advantages and also

can mirror our other approaches to controlling technology outflows. We should not be allowing investors to invest in entities that we have determined we should not be selling those critical technologies to.

But I think the outbound order is taking actually somewhat of a targeted approach, though when it comes to AI, that is going to be one of the hardest issues to get right in terms of how broad do we think about what AI is, what is military use, what is civilian use. These are not easy questions, but I think it is a good start.

Senator MENENDEZ. Well, with intellectual property theft, which remains an acute challenge in our dealings with China, and the theft of intellectual property related to cutting-edge technologies that could seriously degrade our national security and economic competitiveness, I wonder what can we do to expand on the President's order and make outbound investment review a more effective tool for limiting theft of high-tech secrets that are critical to national security?

Ms. GORMAN. It is a good question. I think we can try to tie in some strings to our investments. I think expanding our enforcement capabilities. The DOJ has certainly prioritized the intellectual property theft from China challenge. We need—we need more aggressive enforcement there and to be sure that we are not giving away the crown jewels of our technology through investments, through that transfer of know-how. And I think there is a piece of this, too, that involves communicating to our investors what our priorities are, incentivizing them to make investments in allied partner Nations, not only China, and raising awareness from them on what we are really trying to guard against.

Senator MENENDEZ. Thank you. Mr. Jaffer, it is good to see you. Mr. Jaffer was the chief counsel for the Republicans on the Senate Foreign Relations Committee, and good to see you here. Thank you, Mr. Chairman.

Mr. JAFFER. Thank you, Senator Menendez.

Chair BROWN. Thank you, Senator Menendez. Senator Tillis is recognized from North Carolina.

Senator TILLIS. Thank you, Mr. Chairman. Thank you all for being here. Mr. Jaffer, I am going to submit a couple of questions for the record, but I have tried to explain to people—as late as last night, I had a telephone town hall. People were concerned about China and Chinese investment in the United States, and I tried to explain that some of that is not bad. It is a matter of where they are investing, but what I also tried to explain is how investment in China, not all investment in China is bad. For example, my favorite photo is a little girl wearing a Wonder Woman outfit with a Captain America shield, and she is Chinese. She is at a Disney park in China. Boy, I want as much Chinese investment as we can to export our culture to China, to let the Chinese people see what is possible in the free world.

So how do you—how do we strike that balance and not make it untenable for American businesses to see a market of middle-class Chinese, which is probably shrinking, given some of the reducing in size, but it is still about twice our population. How do we strike the balance as a matter of public policy?

Mr. JAFFER. Yeah, it is a great question, Senator Tillis, and, you know, it seems sort of obvious, but, you know, investing in a tee shirt factory in China is fundamentally different than investing in a semiconductor fab. Transferring technology for, you know, manufacturing that happens at scale of nontechnological capabilities is different than transferring manufacturing know-how for critical minerals or processing for critical minerals. And so there is a commonsense element to the way our investors and our investment community ought to think about investment and business in China. You know, we all made the mistake in the 90s thinking that China being brought into the world—into the—into the, you know—

Senator TILLIS. —toward a democratic, free market framework—

Mr. JAFFER. Right.

Senator TILLIS. —that never occurred.

Mr. JAFFER. We all bought into that, right—

Senator TILLIS. Yeah.

Mr. JAFFER. —from President Clinton to Republicans in Congress.

Senator TILLIS. I did, too.

Mr. JAFFER. And we were wrong.

Senator TILLIS. Mm-hmm.

Mr. JAFFER. China has exploited the—its incentive system. It has taken advantage of it. It is playing unfair ball, and now it is using that repression that it imposes upon its own people and using the free markets to export that repression abroad.

Senator TILLIS. And I am wondering, I think, more broadly, because what we are really talking about here is making sure that China is not successful being the military and economic superpower by 2050, and it seems like if we are really going to talk about that, obviously we have to incent research and development. We have to make sure that the United States remains the innovator that it is today. We have to protect our intellectual property. We have to do everything we can, but it seems like we need to fight on several different levels. It seems to me that the Belt and Road Initiative, you got some buyers' remorse there, but we really have no alternative.

So to what extent are we going to Africa and South America, going to these countries and creating a different value proposition? We do not have to be the lowest cost provider because we know that an American investment, an American framework in these countries means something more, and all of these countries, these leaders get it. So give me an idea. If you could wave a wand and be President for the day, what would be your global strategy, the multilevel strategy to go after China and prevent them from succeeding over the next 25 years?

Mr. JAFFER. Well, I think, Senator Tillis, the first step is we have to be the strongest ally to our friends and the fiercest adversary to our foes. Today, our adversaries are not afraid of us. They know we are afraid to take action in the world, and our allies are not sure we will be there with them.

Senator TILLIS. And so failure. Would you argue that failure in Ukraine is the one thing China hopes happens this year?

Mr. JAFFER. Absolutely.

Senator TILLIS. Yeah.

Mr. JAFFER. Continued attacks by Iran without an—without an effective U.S. response makes China happy. North Korea launching missiles without us doing anything about it makes China happy. These things are not unrelated. China has a hand in all of this. They are working collaboratively with all these Nations. They recognize that a weak U.S., that either appears weak or is actually weak, benefits them.

Senator TILLIS. And do you—I mean, it is topical because of discussions we are having here around the supplemental in Ukraine funding. Do you believe that Putin will be happy and Xi Jinping will be thrilled if we decommit from Ukraine, and then what likely will occur there? I mean, do you—do you think it is in that order, that China sees more to gain from our lack of funding than even Putin?

Mr. JAFFER. Absolutely, and the way you know that is that we saw Xi Jinping stand with Vladimir Putin, and in an aside he knew was being captured by the cameras says to Vladimir Putin, there are changes of the likes of which the world has not seen in 3 decades, and we, Russia and China together, are making those changes happen.

Senator TILLIS. And the last thing—I could talk to you for more than a day—but the last thing there, the fact that China came to the United States, the fact that Xi Jinping came to the United States means that he and the economy and the CCP is on the ropes, right? And when they are on the ropes, you keep them there and you keep them in a corner, and one of the ways you do that is to step up and lead. And I think leadership means that we provide supplemental funding to Ukraine. Thank you.

Mr. JAFFER. Totally agree.

Chair BROWN. Senator Tester of Montana is recognized.

Senator TESTER. I want to thank the Chairman and the Ranking Member for having this hearing, and I want to agree with Senator Tillis' line of questioning, and I appreciate your response, and I want to thank all three of you for your testimony.

Leading is something that is really important. We had an opportunity to do some things in last year's NDAA. The Ranking Member and the Chairman both talked about this. The House blocked every damn thing we tried to do, whether it was a FEND Off Fentanyl bill that we had a hearing on last week that would have held Chinese entities accountable, passed this body by a number that we never get numbers like that, in the high—in the 90s, or whether it was an amendment led by Senator Rounds and myself that would have stopped China and foreign adversaries, the ones you mentioned, Mr. Jaffer—North Korea, Iran, and Russia—from buying farmland, which was also blocked by the Republican leadership in the House. I am going to tell you obstruction, it does not take anybody with a brain to do obstruction, and so if obstructionism is the—is the rule of the day, the House is doing it, and they are doing it really well to the destruction of this country.

I am a farmer. Most people understand that food security is national security. If you want to screw up a company, screw around a country, screw around with their food supply. Recently, we just got a word that a Chinese national bought 200,000 acres of land

in Oregon. We did not know about it. That means our system does not work. It means self-reporting does not work. These folks do not want to self-report, and so we have got some work to do here, but, doggonit, this should not be a Republican or Democrat or House or Senate. This is the United States of America. And so keeping our country safe, not allowing China to spy on us, is really, really important.

There has been a lot of talk about exploiting American innovation here today and it is a fact, and we need to make sure that we stop that from happening. When the—when the spy balloon that went over the United States was shot down, there was some—there was some information that was delivered that they used some technology that was bought in this country. I could ask all three of you this, but I am going to ask Mr. Jaffer. Some of this stuff was pretty simple. Some of it was more complicated than simple. Is there any way to stop this kind of stuff from happening? Is there anything we could do? And after he gets done, if other two would like to respond, you can.

Mr. JAFFER. Well, Senator Tester, you know, there is a spot of hope in the House. You have Chairman Gallagher and Ranking Member Krishnamoorthi, who have done a lot of great bipartisan work together on the China Select Committee to move initiatives forward. Now, there are challenges with leadership and challenges getting, you know, the bipartisan group there together in the House, but there are opportunities, I think, to work and to get some of this stuff done. I think the Nation is waking up to the China threat. You mentioned the sale of certain technologies that end up in Chinese equipment.

Senator TESTER. Yeah.

Mr. JAFFER. You know, it is crazy that American parents buy Chinese drones for their children for Christmas, you know?

Senator TESTER. Right.

Mr. JAFFER. We have got to work to ensure that the American people are well educated about this, and by the way, they are. You go—I was just in Iowa a few weeks ago, and Iowans are worried about what you talk about, the purchase of farmland by Chinese corporations.

Senator TESTER. Yep.

Mr. JAFFER. They are deeply concerned about that, and you are exactly right. I think there are opportunities. The American people are there. It is now bringing our businesses, and our industry, our Government, together with where the American people are to say this is not an acceptable situation. We cannot function in a world in which American technology goes into Chinese spy balloons or Chinese corporations are allowed to buy American farmland, or, frankly, land around our airports, our military facilities, and the like. It is not acceptable. It has to stop.

Senator TESTER. Correct. Anybody else want to respond to that? OK.

Ms. GORMAN. Sure. I would—I would just add I think there is a reason for optimism, and public engagement can go a long way.

Senator TESTER. Yeah.

Ms. GORMAN. One issue that we have tracked extensively, as I know many here have as well, is the issue of information plat-

forms, such as TikTok, operating in the United States. Four years ago, when we raised these concerns, I think we were laughed out of the room. What does—who cares about a meme app? Who cares about cat videos? This is not a national security threat. Today, the most recent Pew Research poll from last year found that now, about 6 out of 10 Americans now view TikTok as a national security threat. That is public education in action.

Senator TESTER. Yeah.

Ms. GORMAN. And so I think there is promise.

Senator TESTER. OK.

Ms. KILCREASE. Yeah. I would just add we keep getting caught short by these sorts of examples—

Senator TESTER. Yeah.

Ms. KILCREASE. —whether it is the spy balloon or TikTok or BGI or whatever the specific Chinese company is, and that means we have got a blind spot in our analytic capabilities.

Senator TESTER. Yeah.

Ms. KILCREASE. We do not understand what is happening in China's technology ecosystems at the level that we should. And so as we think about how to strengthen our tools, you know, that is an area we should be prioritizing. Do we have experts in the Government who have access to both classified information and a wide range of open-source information that really know exactly what is happening inside of China's tech ecosystem.

Senator TESTER. Really quickly, I am a farmer. Self-driving tractors have been around for about 15 years. I finally got to a point where I was going to buy a piece of equipment that would allow that tractor to drive with me sitting in the cab. Every company I called was Chinese, and the people I were talking to was in mainland China, and finally I found an American company, and you know what he told me? He said—I told him what I just told you guys, and he said, yeah, they stole our equipment and remanufactured it. We got to do something about this, and we got to remove the stupidity that is going on over at the House.

Chair BROWN. Thank you, Senator Tester, for—always for your wisdom, born and being a real farmer, so thank you. Senator Hagerty from Tennessee is recognized.

Senator HAGERTY. Thank you, Chairman Brown. On December 20 of last year, Gary Peters and I—Senator Gary Peters from Michigan and I introduced a bill to prohibit U.S. taxpayer dollars from going to companies like BGI that would use this funding to gain access to the U.S. market and, importantly, gain access to American citizens DNA—DNA data, I should say, their genetic data. I want to thank Senator Peters for working with me on this. He is prioritizing this bill for this month's Committee markup. I look forward to getting this passed to deal with this fast-moving threat.

I think all of you know this, that BGI is the largest collector of genetic data in the world. BGI stores this data in China's National Gene bank, which is directly managed by BGI, and it is owned by the Chinese Government. BGI has analyzed some of this data that it has collected using supercomputers that are built and operated by the Chinese military. What concerns me here is not just the collection, the storage, and the analysis of this highly sensitive data.

It is also China's ability to use this trove of biological data and other life sciences data to train advanced dual-use artificial intelligence models, perhaps for malign purposes.

So, Ms. Gorman, I am going to start with you. The question has two parts. I have heard from many AI professionals regarding the risk of China having access to massive life science training data. What, in your opinion, is the greatest national security concern regarding BGI's access to this, and what could the Chinese Government do with troves of U.S. genomic and other life sciences data when you couple it with advanced AI models?

Ms. GORMAN. Senator, thank you for the question. Really, thank you for your leadership in raising awareness of these issues on genetic data and genomic data. I think there are a number of maybe doomsday scenarios that experts would point to—personalized bio-weapons, for example—that could be designed. What I am more concerned about are two things. One, that these—DNA information is some of our most sensitive information, and we already know that the PRC has an ethnic mission to remake its population in favor of its Han Chinese population and is committing massive human rights abuses on its ethnic Muslim populations, like the Uyghurs. DNA surveillance can put that on steroids.

Senator HAGERTY. Mm-hmm.

Ms. GORMAN. Second, there is a competitiveness worry here. These technologies are the future. Personalized medicine, individualized medicine combining biotechnology and artificial intelligence, these are where our future therapies are going to come from, and I do not want them to come exclusively from China.

Senator HAGERTY. Mm-hmm.

Ms. GORMAN. So I worry that they are amassing these data bases, and we—because we will not collect DNA on our own citizens, and nor should we, we might fall behind.

Senator HAGERTY. And this is to any of you that want to respond to this, but what do you think Congress should do to prevent China from gaining access to this type of life sciences data that could be used to train dual-use AI models?

Ms. KILCREASE. You know, I think there are a range of tools that Congress could consider. It is worth just emphasizing a point that Ms. Gorman made. You know, genomic data is particularly sensitive. If somebody steals my password, I can change my password. I cannot change my genomics or my genes, you know.

Senator HAGERTY. Yeah.

Ms. KILCREASE. And so we should be looking at a heightened level of sensitivity—

Senator HAGERTY. Mm-hmm.

Ms. KILCREASE. —and a heightened level of protection precisely because of the unique nature of this sort of data. So a range of things that we could think about, certainly U.S. taxpayer dollars should not be going to support the growth of Chinese national—

Senator HAGERTY. Agreed. Yeah.

Ms. KILCREASE. —champions in this space, of course. We should be thinking about their access to our U.S. domestic market. You know, a weak spot in our economic security toolkit is Chinese access to the U.S. domestic market. That comes up in the ICTS space. It certainly comes up in this space as well.

Senator HAGERTY. Senator Peters and I are trying to get at that, yeah.

Ms. KILCREASE. Exactly. The last point I would add is there is a broader conversation about the bulk transfer of any sort of sensitive U.S. person's data overseas to foreign adversaries. We simply do not have a legal authority that allows us to prevent that, and that is a real national security risk.

Senator HAGERTY. I think we should take a hard look at that. I would like to stay with you, if I might, Ms. Kilcrease. I want to shift gears to talk with you about Nippon Steel's proposed acquisition of U.S. Steel. You have publicly stated that you would be shocked if the deal got blocked. You are a former senior staffer at the Committee on Foreign Investment in the U.S., CFIUS. Could you walk us through the foreign investment review process and explain why you believe the deal would be unlikely to be blocked for national security reasons?

Ms. KILCREASE. Sure, and I will focus my comments really on the CFIUS legal framework and how CFIUS typically views risk assessments in these sorts of transactions.

You know, CFIUS, under its mandate from Congress, is laser focused on national security risks, but its concept of national security can be flexible. It can include economic factors, and so for a transaction like this that involves a critical component for our defense industrial base, I would expect that they would be looking—certainly, first of all, they will—they will look at the deal, right? It is a big deal, it is a significant deal, so there is an interest to review the deal in the first instance.

But as they are thinking about risk, they will be looking at how the transaction would affect domestic production and domestic availability of steel, particularly the sorts of steel that are important for our national security platforms. They may also be looking at the workforce available to support that continued production. If there is a problem there, CFIUS has a range of authorities it can use to impose mitigation terms on the deal. That is typically how CFIUS in past practice has addressed those sorts of economic related concerns, to the extent that they rise to the level of a national security risk.

Senator HAGERTY. Can you apply them to this instance then?

Ms. KILCREASE. So with the caveat that I do not have access to all of the deal information, you know, my sense is that if they did think that the acquisition was likely to lead to these negative sorts of impacts on U.S. domestic steel production, that it is very possible that there would be a mitigation agreement that would be either negotiated with or imposed on the companies to address those and to make sure that those are not those negative impacts. You know, the comment that I made that you quoted that I would be shocked if the deal actually got blocked is simply because we typically—CFIUS typically does not block those sorts of deals or does not recommend that the President block those sorts of deals based on past practice. The fact that it is Japan and not China making the acquisition, I think, will be relevant in their consideration. I think there will be an incentive to, you know, consider the alliance aspect in their review as they move forward.

Senator HAGERTY. Thank you. Thanks, Mr. Chairman.

Chair BROWN. Thank you, Senator Hagerty, for exploring that. Senator Warren—Warner from Virginia is recognized.

Senator WARNER. Thank you, Mr. Chairman, and thank you for having this hearing, and, Ms. Gorman, it is good to see you. I will quickly address one of the things you mentioned about TikTok. I do think it is a national security concern. I think we have—it is remarkable, though, what the power of money buys in this town. When we had broad-based bipartisan support on a comprehensive approach that would not only take on TikTok, but a framework for threatening technology from adversarial Nations, it was—almost looked like it was going to be too easy at first. We had 26 senators evenly divided, support from the Administration, support from lots of industry, to have this organized approach so it would not be a one-off. ByteDance then dropped \$100 million on getting folks from the far left and the far right to come out against our approach. They literally bought up advertising. Every political tip sheet in D.C. was sponsored by—for weeks on end by TikTok. And I think this problem has not gone away, and we need to revisit it now more than ever as we see TikTok, and, unfortunately, I think the CCP play out their agenda using TikTok because it is a news delivery model.

I want to talk a little bit, though, about another area on open source. Open source has played a huge role in things like software development for years. We have seen it play a role in semiconductor architecture, AI models, AI development models. It is one of the reasons why I have worked with Senator Kennedy on this Committee on a bill, Senate Bill 3554, the Financial Artificial Intelligence Risk Reduction Act, that goes after some of the challenges around AI in the financial markets where I think we have huge, huge vulnerabilities. I want to get the plug in on my bill, and I am come back to open source. Now, you know, there is a lot of value in open source, but I have been—when we look at some of the projects, like the RISC-V initiative, how the PRC is using that in the semiconductor area to gain information.

And maybe just go down the aisle, starting with you, Ms. Kilcrease. How do we—how do we do—you know, there is value in open source, there is a lot of good research going on in open source, but how do we better educate American companies that, many times through some of these open source projects, we are basically giving away the crown jewels for free. I can tell you, sitting from the—Chairman in the Intelligence Committee, we see China prey upon these open-source opportunities all the time. How do we do a better job of getting companies to understand that risk? And I will take of—each of you.

Ms. KILCREASE. Thank you for the question. It is a really hot button issue in certainly the chip space and in the AI space right now about how to think about open source models. You know, it is important to recognize upfront that this is exactly the kind of tactic that China would use to circumvent ever-increasing levels of controls. If they cannot get the chip directly, if they cannot access controlled design technology, they will, of course, look for what is available on the open market through either licit or illicit means.

Now, there are benefits to the open source approach, and certainly some of the safety researchers will tell you that there are

some benefits to having the public being able to access and test these sorts of open source models. However, it really does depend on who is doing that, right? And as we think about trying to make these tradeoffs and these balances, I do think we need to have a more serious conversation on controls, on the release of some of these models, particularly the really powerful frontier AI models, where we do not even know what those things are capable of yet.

Senator WARNER. Mm-hmm.

Ms. KILCREASE. And so whether that is putting parameters around AI models with a certain computing power, compute function, really just trying to put in place some commonsense guardrails that maintains a level of openness so we can get those innovation and public safety benefits while also making sure that those sorts of models do not go to adversary countries.

Senator WARNER. Mr. Jaffer.

Mr. JAFFER. Thanks, Senator. Look, I think there is a challenge when you think about putting the kind of restrictions on that we are talking about, this idea of open source models that have a certain size or certain compute power. We do not know what those technologies can do, but we also do not know the benefits they can offer us. So I think artificially limiting those ahead of time could be a mistake. I think the right approach instead is to take a more comprehensive look across the board and realize that our system benefits from having both open source capabilities out there as well as private proprietary software, and that we work best in an environment where both operate in parallel, and there are open source capabilities that are out there.

Those tend to be less powerful. You will find the proprietary models will likely be more powerful and more capable, and, ultimately, because they are able to make more money off those, will be able to sell those at higher rates. And so you will see more investors, I think, head toward proprietary capabilities, but shutting off the open source environment, I think, would be a mistake, just like putting artificial constraints on models based simply on their compute power and the like.

Senator WARNER. —necessarily shutting off, but I am thinking we ought to be going eyes wide open.

Mr. JAFFER. Absolutely.

Senator WARNER. And I fear sometimes some of the companies involved do not recognize that. Ms. Gorman.

Ms. GORMAN. Senator, it is great to see you, too, and I agree that heading into this historic election year with the TikTok election is disastrous. On the open source question, we have to take it back to what are our national security objectives, and here, I would actually put forward that we should look at the applications. We are going to see specialized models that are application-specific large language models. Processing text is just but one of these examples. We are going to see the large language models for our immune system, the large language models for manufacturing data. Which of those application areas have a national security sensitivity that we do not want that to be open source?

And I would also add that there is an advantage of open source beyond just our innovation advantages, but there is actually a strategic advantage, which is that we benefit from the fact that GitHub

and open-source platforms and software engineering, they are written in English. That English is the lingua franca of software development, and Chinese engineers publish in English. I do not think we should cede that advantage, as well, because China is also developing their own open-source models and open-source platforms and data bases, and that is actually an area for competition as well.

Senator WARNER. Thank you. Thank you, Mr. Chairman.

Chair BROWN. Senator Vance from Ohio is recognized.

Senator VANCE. Thank you, Mr. Chair, and thanks to you and Ranking Member Scott for hosting the hearing, and thanks to the three of you for being here.

I want to direct my questioning to Ms. Kilcrease. In particular, I want to ask you about a live situation, the Nippon Steel acquisition of U.S. Steel and something that I know a number of my colleagues from both sides of the aisle have expressed some concern about, and I have shared in those concerns. In fact, I wrote a letter months ago, worried that the U.S. Steel board would entertain foreign bids, even though I think it is a bad idea for a host of reasons we can get into. But, you know, but one of my concerns here is that the interest of foreign bidders in U.S. steel is not primarily about green fielding investment into the United States of America. They are not expanding steel production domestically, and they are not necessarily doing it because they have better access to capital. They are doing it primarily as a sort of tariff arbitrage. They are effectively buying access to the domestic markets in a tariff-free way.

And, you know, I think that in a—in a world where, first of all, we are talking about one of the most protected industries, steel, in the world, pretty much every country that has a steel industry has significant protections placed on it. And we have learned the hard way over the last couple of years that America's capacity for manufacturing in some of the most critical weapons and other things is actually pretty lackluster, given our needs. I worry about what this means for our country, and I just want to ask, you know, this question. So am I right, Ms. Kilcrease, that the only real tool or the only real organization that could review this transaction would be CFIUS?

Ms. KILCREASE. That is right. CFIUS is the one that would review this foreign investment consistent with its national security mandate.

Senator VANCE. Right.

Ms. KILCREASE. There may be antitrust as well, but it is basically CFIUS—

Senator VANCE. And we are expecting a CFIUS review on this particular transaction, correct?

Ms. KILCREASE. We are, and there have been public statements to that effect, yes.

Senator VANCE. Got it.

Ms. KILCREASE. Yeah.

Senator VANCE. So here's my question.

Ms. KILCREASE. Mm-hmm.

Senator VANCE. CFIUS is primarily or maybe exclusively a national security standard that it applies to reviewing these trans-

actions. Can CFIUS consider public interest concerns as part of its review?

Ms. KILCREASE. It cannot. So CFIUS is a national security test. It is a broad and flexible concept of national security, but if the concern, for example, is whether foreign investors are trying to get around tariff structures, it would be unusual for CFIUS to take action on that basis. And we probably do not want to encourage the bureaucracy to kind of get outside the four corners of the legal mandate it has been given by Congress.

Senator VANCE. Yeah, I agree with that. I guess part of my question is whether the—that we think that the four corners’ legal mandate here is a little too narrow for what we are concerned about and what we are interested in.

Ms. KILCREASE. Mm-hmm.

Senator VANCE. What do you think—I mean, if we wanted to empower our Government to, you know, ensure that we had things like sufficient native domestic production of steel, what do you think we might—maybe should do here? You know, if you were sort of, you know, legislator for a day and we wanted to further empower the Congress to protect, and I use that word intentionally, the domestic steel industry, what do you think we should be doing differently vis-a-vis transactions like this one?

Ms. KILCREASE. So if there was a desire to have authorities on more of a public interest test for our foreign investment reviews, certainly that would require additional legislation. That is a gap. If the policy objective is to protect those sorts of domestic industries, apart from distinct national security concerns, we do not have a tool to do that today. So you would certainly want to consider whether there is a need for additional legal authorities as well as considering the impacts more broadly on downstream industries and broadly across the economy for that sort of proposal.

Senator VANCE. Great. I appreciate that, and, you know, maybe my office can follow up on some ideas on that front because I do think it is important. And I know just on this point, just to pontificate a little bit, there has been some concern, some pushback on my view that, you know, you should not be worried about Nippon Steel buying U.S. Steel because Japan is an ally, and Nippon Steel appears to be a very good company. I do not disagree with that. I think it is important to sort of point out that the Japanese are—you know, it is a great, great people, and they are an important ally.

They also are fundamentally in the sphere of influence of China. You can imagine a scenario where domestic steel needs would fall by the wayside when you have an international company that owns those—that owns those rights and owns those production mandates. So just because they are an ally, I think, does not mean we should not be concerned about a foreign competitor buying up one of the most important industries, one of the most important companies for a very, very critical—not just national security, but full American interest company. So with that, I will yield, and thanks to the Chairman for giving me some time.

Chair BROWN. Thank you, Senator Vance. Senator Cortez Masto from Nevada is recognized.

Senator CORTEZ MASTO. Thank you. Thank you, Chairman, and I want to thank the Chairman and Ranking Member for another incredible hearing today on an important topic. All three of you, thank you, for giving us pause to question where we need to move forward and where the gaps are and what is working well.

Let me—and let me, Mr. Jaffer, start with you because I could not agree more. We have got to start thinking, we bring those jobs back here, we bring the manufacturing, the processing back here. Here is an area that, for me, and I am from a mining State, the State of Nevada, and I have watched China as they have cornered the market on mining, and China currently controls about 90 percent of global rare earth mineral processing and rare earth magnet manufacturing, and that was not just by chance, right?

Last month, China announced an export ban of rare earth extraction and separation technologies. Between this action and its recent export ban on other minerals, like graphite, gallium, germanium, it is clear China is threatening to weaponize areas where it has dominance over critical supply chains. For the benefit of the public if they are listening, there is not any rare earth mineral mining, except maybe one place, and that is Nevada and California. So that is why Senator Mullin and I have legislation to strengthen the domestic rare earth magnet supply chain and bring that extraction, the processing, manufacturing of these critical minerals, back here to the U.S. I hope my colleagues join us in this legislation.

But my question to you is, how should the U.S. be thinking about our own export controls in light of these moves? We have had conversation. What else have we not talked about today?

Mr. JAFFER. Well, you know, Senator Cortez Masto, I think it is critically important the issue you raised, this idea of critical minerals, strategic metals, rare earths. The fact that we do not have access to those here in the United States, the fact that we could get access to it, but our own environmental laws, our own—our own willingness to move our policies in the direction of making ourselves independent from China on those, is part of the problem, and it is not just the actual minerals themselves. Even when those minerals come from abroad, we cannot process them here because we do not have the capabilities. Our environmental laws and other laws make it hard for us to do that in the United States. We have got to incentivize businesses to engage in both mining extraction and processing here in the U.S. if we are going to free ourselves from this capability.

And then going beyond that, I think that what we have to realize is that, to your point, this was not a mistake. This was not by accident that China ended up with a—with a huge portion of the world's capabilities in processing and obtaining and extracting minerals. They are making these moves in a range of other industries as well, whether it is semiconductors, access to data, artificial intelligence and the like, high-performance computing, accelerated computing. We need to be—recognize that China is strategic. They have a 2030, 2050, hundred-year view of the world. We operate, and what makes us so innovative is we operate on a every month, every year, every quarter view of the world, and that makes U.S. rapid and innovative.

At the same time, we have to recognize that we are contending with an adversary that has a generational view of the problem. We need to take a generational approach. That means working closely with our allies. It is onshoring and ally shoring, and recognizing that our allies have a choice to make. If Europe is not with us, they do not succeed. They need to understand that Europe coming after American companies is a huge mistake. It does not benefit us, it does not benefit them, and it harms all of us in the long run against China.

Senator CORTEZ MASTO. And would you agree that China is taking advantage of the partisan bickering that is happening in Congress right now?

Mr. JAFFER. One hundred percent. The partisan bickering happening in Congress and the partisan bickering happening in our country.

Senator CORTEZ MASTO. Yeah.

Mr. JAFFER. The fact that we are divided as a Nation on issues like Ukraine, on issues like Israel, on issues like America's role in the world is a benefit to China. We need to get on the same page. It needs to be America leading the world, and it needs to happen as soon as possible.

Senator CORTEZ MASTO. I agree. This is—this is for the panel because there is another area, and I so appreciate this conversation. It is a challenge for us to, quite honestly, get anything done, right? There are some good things that we have talked about that we have done. There is more that needs to be done. Let me just bring one of them to you and get your thoughts on this. This is the idea of privacy.

So the director of the White House's office of Science and Technology Policy said that Federal privacy legislation must work in harmonization with Congress' forthcoming legislation to create guardrails on artificial intelligent development. We are having this conversation about AI. I absolutely agree we need guardrails, we need to figure this out, but there is an idea that we also have to address privacy, privacy and security. Now, I have legislation that I have introduced 4 years ago. There is legislation out there my colleagues have introduced on privacy and security. Has not passed. We have not moved forward as we have watched some States do it. We have watched European Union.

So I guess my question to all of you is, how important is it for us not just to address the AI and the challenges we are facing there, but also address this idea about privacy and privacy data and security? Would you agree that they need to be harmonized?

Ms. GORMAN. Yeah.

Ms. KILCREASE. Absolutely. Oh, sorry. Go ahead.

Ms. GORMAN. No, go ahead.

Ms. KILCREASE. It is such a huge national security risk. You know, as you think about the future that our children are growing up in and the lives that they are living online, and the fact that that is data that can be scooped up and sold to the highest bidder, it is terrifying. It is not in the public interest. It should be a high priority for Congress.

Senator CORTEZ MASTO. Mm-hmm.

Mr. JAFFER. I think there is a real call to do something on privacy. I think the challenge is we need to avoid making the mistakes the Europeans made. They passed comprehensive privacy legislation. Everyone says we are behind Europe, but the reality is that our innovation system functions because we are not passing the kind of overweening, over regulatory laws that the Europeans are doing. In their privacy laws, they made it harder to achieve noble and novel cybersecurity initiatives as well. So we have got to make sure we act—we act, you know, cognizant of the implications some of these laws might have.

It is a problem that we have various States doing this. We are going to need Federal comprehensive legislation. The question is, what does it look like and what does it need to do, and what national security interests do we need to account for in that, including our ability to collect foreign intelligence in the United States, you know, an issue which is now before the House and the Senate, expiring here in April, critical legislation that we need to pass and get back into law.

Ms. GORMAN. Yeah, privacy is a core democratic value. It is the bedrock of freedom of expression and assembly. It is a travesty that we do not have Federal privacy legislation, and it exposes us to other data security risks with some of these Chinese ICTS platforms that are exacerbated by our lack of a baseline protection of individual data. I would also add in the AI conversation, there are technologies that are in development that would actually allow us to help preserve some of that privacy. I am talking about privacy-preserving AI, privacy-enhancing technologies, where with AI, the issue is that the best AI models are trained on massive, massive amounts of data, and that is inherently, when it is personal data, a potential privacy violation. But there are technologies in development that would allow us to train these models without compromising the privacy of individual data, and I think we need robust investment in the advancement of those capabilities as well.

Senator CORTEZ MASTO. Thank you. Thank you, Mr. Chairman.

Chair BROWN. Thank you, Senator Cortez. Senator Britt of Alabama is recognized.

Senator BRITT. Thank you, Mr. Chairman. Thank you to all of our witnesses for being here today. Mr. Jaffer, as a former staffer to a former staffer, welcome.

We continue to be reminded of the national security and economic implications of the Chinese Communist Party and the threat that they pose both to our country and to our future. Time and time again, the CCP has shown that they are not willing to play by the rules that govern international commerce. They have aided and abetted Iran, evading U.S. sanctions, and they are actively stealing U.S. technology and intellectual property across whole sectors of our economy, from artificial intelligence to computing to robotics to biology and beyond. In fact, the FBI's economic espionage caseload related to China has increased approximately 1,300 percent over the last decade. Today, on average, a China-related counterintelligence investigation is opened every 10 hours.

The stakes could not be higher, and we must ask now to mitigate the ongoing economic harm happening to hardworking American families, Main Street small businesses, budding entrepreneurs, and

critical industries. To that point, we must stop the CCP from buying U.S. land. Not only is this impacting the availability of fertile farmland for our agriculture community, but the CCP has deliberately compromised national security by purchasing land near our military installations. So I am proud to have joined Senator Tom Cotton in introducing the Not One More Inch or Acre Act, and I continue to urge my colleagues to join this effort.

The U.S. has also—looking at existing tools that protect our national security and safeguarding technology innovation happening on college campuses and research and development labs and facilities across the Nation. We have taken a look and we are looking at what the CCP is trying to do to undermine those things. The Committee on Foreign Investment in the United States, in addition to export controls, classifications and security clearances and sanctions, all contribute to the firewall protecting American innovation, American IP, and American research from the Chinese Communist Party and other nefarious actors.

Mr. Jaffer, I would like to ask you, where are the gaps in our current toolbox, and how do we ensure that U.S. security capabilities are able to keep up with evolving tactics by—and technologies that are being deployed by the Chinese Communist Party to steal our cutting-edge, our groundbreaking technology, the research and innovation that is happening here in the U.S.?

Mr. JAFFER. Yeah. Well, Senator Britt, I think there are a few things we could do to help staunch the flow of U.S. intellectual property out the back door. One, we have got to deter effectively the Chinese. That means taking the fight to them, right? We have allowed the NSA and our—and our Cyber Command to get more aggressive and to lean forward to defend forward into adversary networks. More needs to be done there. We need broader authorities to allow our Government to push back more aggressively. We need to take the policy decisions to actually push back against Chinese depredation and the—and the efforts that other Nation-State actors, like the Iranians and Russians, are doing on our networks as well.

Second, we also need to ensure that we have the policies and procedures in place that allow us to effectively push back economically against the Chinese. Today, we use tools like the SDN List, the Enemies List. These are not tools that are designed for the kind of economic depredation they engage in. We have either a sledgehammer on one side or a scalpel on the other. Neither works. We need a butcher knife that requires action by Congress to give the Administration more tools, and then the Administration needs to use those tools and use them effectively. Simply designating a group like the Houthis as especially designated global terrorists and not using the FTO designation is a mistake.

Senator BRITT. Could not agree more.

Mr. JAFFER. Exactly. And so—and so we need to be more aggressive, and it is not just in capabilities and tools. We have to use them more aggressively. We have gotten too used to only using economic tools. They are not as effective as they could be. We need to get more aggressive on that front as well.

Senator BRITT. Listen, while we are talking, I know I only have less than a minute. I want to talk a little bit, transition a little bit

into BRICS. When I am looking at what I am—I am seeing, obviously, we have had four more countries. We saw four more countries join earlier this month. Over 40 countries have expressed interest in joining BRICS, and 22 of them have formally requested membership. I think this is startling and concerning, and I think, America, we need to wake up, and I think we need to demand that people withdraw from BRICS. And my question to you is, in your opinion, has the U.S. adequately examined the consequences and economic concerns and potential national security implications of BRICS, and what more do we need to be doing to push back on this?

Mr. JAFFER. We have not done nearly enough, and the reality is that we are in something of a cold war today with China, right? We have to view the Chinese effort to consolidate its influence and authority over Nations in our own hemisphere, as well as in Africa and around the globe, as a strategic threat to our ability to continue to lead the world. And that comes from us being a strong adversary to our foes and a strong ally to our friends. Nobody trusts the United States today. They do not trust that we are going to be there.

They saw what we did to our allies with the Kurds under the prior Administration. They saw what we did to our allies in Afghanistan under the current Administration. They have seen it over and over again. They see our adversaries punch at us, with Iran, with China, with Russia, and they see U.S. take those punches and do little to confront them. Until we demonstrate that we are prepared to lead and be a good ally to our friends and a real adversary to our foes, nobody is going to come alongside us, BRICS will continue to grow, China will continue to gain influence, and countries in our own hemisphere will switch their recognition from Taiwan to China. It has happened twice in the last 6 months.

Senator BRITT. Yep. It is a huge strategic threat.

Chair BROWN. Thank you, Senator.

Senator BRITT. So thank you so much. I appreciate it.

Chair BROWN. Thank you, Senator Britt. Senator Warren from Massachusetts is recognized.

Senator WARREN. Thank you, Mr. Chairman. Every time you log onto a website, Big Tech companies collect extremely detailed data about your spending habits, your physical location, your health status, your political beliefs, your religious beliefs, and more, and every 30 seconds, Big Tech companies auction off that data to the highest bidders here and around the world. Now, Americans' data are broadcast in this way 107 trillion times—that is trillion with a "T"—every year. This does not just pose a risk to Americans' privacy. It also poses a risk to our national security. Reports have found that some buyers of our data build huge dossiers of extremely personal information about U.S. Government officials and military service members. They then turn around and sell that information to companies in China and Russia, where the Chinese and Russian Governments can access it without our even knowing anything about it.

Ms. Kilcrease, you have spent years in Government service working on issues like data security policy. So when China or another

foreign Government gets their hands on our data, what can they do with it?

Ms. KILCREASE. Well, nothing good comes out of that situation, Senator Warren, so thank you for the question. There are a range of national security risks that can arise from the unfettered transfer of that sort of information on U.S. citizens. To take one example, there has certainly been public reporting about Fitbits on U.S. soldiers being used to enable the movement of our troops. That is a clear national security concern.

Senator WARREN. Uh-huh.

Ms. KILCREASE. And when you think about the types of personal information that is available online and can be collected and sold, as you note, you can think about enabling blackmail. You can think about enabling cyber exploits. It is just a massive counterintelligence concern, essentially, when that level of information is for sale on the open market about individuals who are in these sensitive positions.

Senator WARREN. But Big Tech tells us that it is helping us when they sell or store your data however they want, wherever they want, because it will improve your online shopping experience, or they claim it will help keep your data safe. In reality, the only winners are foreign Governments and the tech companies themselves. Harvesting more of your data means you get more targeted ads, and Big Tech gets more revenue from those ads. And as part of the bargain, foreign Governments, our adversaries, get access to compromising information about U.S. military and Government personnel and their families.

Now, Congress and the Biden administration have plans to address those risks, and Big Tech companies know this. That is why they are hijacking our trade agreements to slip in provisions that would prevent policymakers from limiting Big Tech's ability to transfer our data wherever they want. Now, the Big Tech lobby likes to say, do not worry, Congress could still act to protect Americans' data under certain exceptions, like, if there is a, "legitimate policy or national security need."

Ms. Kilcrease, in theory, the exceptions that Big Tech companies want us to rely on would give policymakers some ability to override the data provisions that Big Tech slips into trade deals, but of the 48 times that countries have invoked a public policy exception at the World Trade Organization to protect their domestic policies, how many times has it actually worked?

Ms. KILCREASE. You know, I think when those sorts of public policy exceptions are raised in the WTO context, not speaking for when the U.S. Government raises it because, presumably, we are always acting with legitimate public policy and national security interests in mind.

Senator WARREN. Uh-huh.

Ms. KILCREASE. But I understand that the number is fairly limited in terms of the ability—

Senator WARREN. Do you happen to know the actual number?

Ms. KILCREASE. I believe it may be two, ma'am.

Senator WARREN. Two. So twice out of 48 times this exception has actually been worked. Just 2 times. I got to say, I do not like our chances on using this exception, and the national security ex-

ception is no more reliable. Trade law tribunals have consistently ruled against the U.S.' use of this exception. Unaccountable trade tribunals should not decide who gets access to information about American soldiers and about our national security, and Big Tech companies cannot be allowed to co-op trade policy for their own benefit, especially when that means continuing to allow the Chinese and Russian Governments easy access to personal data about U.S. Government officials in our military, putting our national security at risk. American data policy should be decided by the American people through their representatives right here in Congress, not by trade tribunals, not by trade negotiators, and certainly not by Big Tech. Thank you, Mr. Chairman.

Chair BROWN. Senator Warner, thanks. Senator Reed of Rhode island is recognized.

Senator REED. Thank you very much, Mr. Chairman. I thank the panel for being here. Ms. Kilcrease, unlike other financial institutions, private equity funds and hedge funds are exempt from requirements to maintain anti-money laundering programs, verify the identities of their customers, and report suspicious transactions. Are you concerned that this opacity of the private market presents a national security threat?

Ms. KILCREASE. Absolutely, and thank you for that question. I think it has been recognized for quite some time, including dating back to at least 2015, that there is a potential loophole in our ability to enforce sanctions when it comes to these particular pools of money. And as we are increasingly imposing larger levels of sanctions, including the historically large and unprecedented waves of sanctions that we have imposed against Russia in response to its invasion of Ukraine, those sorts of bad actors, those sanctioned actors, they are going to look for end runs. They are going to look for legal ways to continue to access their money. So I do think it is critically important that we take a hard look at these sorts of evasion routes and these sorts of loopholes to make sure that when we impose these sorts of sanctions, they are really biting the way we want them to.

Senator REED. Well, and there is another aspect, too, and that is, particularly when it comes to China and Russia, the ability through these private arrangements to conduct espionage, to get access to technology or secrets or plans because they are part of the enterprise. Is that a concern of yours also?

Ms. KILCREASE. You know, it certainly could be. If they are having access to these sorts of investment funds and the funds are then investing in U.S. critical technology companies, I mean, that is the exact reason why we have CFIUS, is to make sure that those sorts of financial transactions cannot be used to access sensitive information that would be contrary to U.S. National security interests. But what you are raising, of course, is a really critical question around whether we have visibility into these sorts of transactions and the right ability to enforce, and I do think that is an area where we need to continue to have a really strong focus to make sure we are shutting down all those sorts of loopholes.

Senator REED. Speaking of CFIUS, Ms. Gorman, when the last reauthorization came about, I included a provision that directed the Committee on Foreign Investment in the United States,

CFIUS, to establish a process to assist partners and allies with foreign investment review, basically to collaborate with foreign agencies and look closely at what was going on. And last May, Assistant Secretary Paul Rosen described how CFIUS is working now with more than 20 other countries to pool their investigations. Should Congress provide a similar statutory mandate to coordinate export control authorities, resources, and information sharing with partners and allies?

Ms. GORMAN. Thank you, Senator, for that provision and your leadership on that issue, and it has been inordinately successful. In the European Union, we have gone from 11 Nations having inbound investment screening regimes before the provision to now 21 after, and more and more Nations are working to set up their own investment screening mechanisms. So I think that, yes, that type of provision where Congress provides the authorities, the resources, and the coordination mechanisms, and, crucially, that—those authorities to share some of that sensitive information with our close allies and partners would be the next step that is needed in our export control frameworks because these controls will shoot us—shoot ourselves in the own foot if they are not done multilaterally. We have heard from U.S. industry that they want multilateral controls, and they have the effect of not actually preventing the technologies from getting into the hands of the PRC. So the best thing we can do is fully resource, create these longstanding mechanisms of collaboration, and I think the FIRMA is a great one to use.

Senator REED. Finally, Ms. Kilcrease, we were all very excited after being shocked by the Russian invasion of Crimea—not Crimea, but Ukraine—when it appeared that our export controls and other sanctions were having a tremendous effect on the Russian economy, but it appears they have been very successful evading those controls, and their economy now is not the critical issue. It is weakened, but it is not the critical issue. What more must we do to make sure our sanctions are effective?

Ms. KILCREASE. Yeah, it is such an important question. Thank you for that. A lot of it comes down to enforcement. We just need to pour more resources into making sure that the inevitable efforts to get around our sanctions and invade our sanctions, that we have got export control officers who are robustly looking out for that, but also, we need to be putting a lot of diplomatic pressure onto some of these third-party countries that are key sources of transshipment. The trade data consistently shows that there is just a massive amount of particularly Western components going through countries like Turkey, like the -Stans through China and getting into Russia and ultimately ending up on the battlefield. That is an unacceptable outcome. We really need to be putting pressure diplomatically on these countries to take action in their own jurisdictions to align with the U.S. sanctions approach, or, ultimately, we are going to have to take enforcement actions on many more companies in those countries to really crack down on this sort of evasion.

Senator REED. Thank you very much.

Chair BROWN. Thank you, Senator Reed. Senator Van Hollen of Maryland is recognized.

Senator VAN HOLLEN. Thank you, Mr. Chairman. Thank all of you for your testimony. It is an important conversation, and, of course, the title of the hearing is, "The Challenge of Outpacing China in Emerging Technologies". And I would say, first and foremost, we have got to invest here at home in making sure that we remain at the cutting edge. The CHIPS and Science act was a big part of that. The chips part of that was funded. The science part was authorized and remains unfunded. It seems we have really got to invest in those areas, everything from AI to quantum computing to other areas. Second, I do want to mark in terms of protecting U.S. intellectual property, Ben Sasse, former senator, and I teamed up. We introduced and we passed legislation entitled, Protecting American Intellectual Property Act, which does give the executive branch more tools to help companies who are victims of intellectual property theft by China or anybody else.

Third, I want to pick up on the conversation we just had with Senator Reed but also to say I do think the Biden administration has taken the right approach overall. They recognize that we are not going to decouple from economic engagement with China, but they also recognize that we have to de-risk, and we have to make sure that we de-risk critical supply chains, and that we have to work with our partners in preventing very high-end technologies that can be used for military purposes from getting to China. And as you know, we have done that in the area of some very sophisticated chips, manufacturing equipment with this trilateral agreement we reached with the Netherlands and Japan, and we need to build on that. As the Administration says, small garden but tall walls. We want to protect sort of our crown jewels and technology, and we want to—but to have the tall wall, and I want to pick up on the conversation on multilateralism and having cooperation of our friends and allies and other advanced economies in this—in this effort, and especially with respect to where we are going on AI right now because I believe we need—we need a multilateral approach. We need an export regime with our allies, similar to the CFIUS process, which has grown and developed.

When it comes to AI, Ms. Gorman, as you know, the Europeans have moved forward with some regulations. Do you see that—the fact that the United States and the European Community are not right now on the same page or the same place as creating openings for China in terms of trying to set standards for AI or to advance their own interests in that area?

Ms. GORMAN. Thank you for the question. I think yes and no. I have heard conversations from folks in the community who are talking about how China is regulating AI better than the U.S. is. I think that is totally wrong. China has staked out a position on AI regulation, but it is in its own national security interests, promoting its own core socialist values. So I think we should strive toward transatlantic alignment on AI regulation and AI use. I do not think that means we are going to be doing the same thing.

I like the innovation-forward approach that we have taken so far, making smart investments in responsible AI development use, privacy protecting technologies in AI, and then agreeing on some of the common guardrails and baselines. For example, using AI for social scoring and mass surveillance, that is a clear no. The U.S. and

the EU have both said that. Let us build that into our approaches. I am also really worried about the threats of AI to our electoral processes when it comes to disinformation and deepfakes. I think there are issues that we can really agree on and put forward multilateral, democracy-forward regulations on AI without having to be completely in lockstep with the EU.

Senator VAN HOLLEN. Yeah. No, I am not suggesting that we adopt what the EU has done, but I—it is another area where more coordination, it seems to me, could be helpful. In terms of protecting high-end chips technology, there has been this new sort of open-source RISC-V technology. I do not know if any of you are following this story closely, but it is an open source, and there is increased reporting that China is actually drawing upon some of this open-source technology for their own semiconductor development purposes. I do not know if any of you can comment on that because as we talk about trying to, you know, coordinate among our allies and friends, obviously, if there is a back door through open source, that could create issues. Ms. Gorman.

Ms. GORMAN. Yeah. I would just say that we have to be smart about which initiatives and which technologies we want to really try to open source. There was a movement in electronic design automation software some years ago to try to create open-source repositories for creating these kinds of designs, but when we actually looked at the competitive analysis landscape, it turns out the U.S. has massive advantages in concentration of market share in these EDA software technologies. So this is why our lack of an analytical capability continues to harm us—because we cannot assess the effects of should we build out a robust open-source ecosystem in something, or is it going to sacrifice some of the critical chokepoints or advantages that we have? And without that capacity, I think we are flying blind in a number of these areas that are central to our future AI competitiveness.

Senator VAN HOLLEN. I appreciate that, and I see time is out, so I am going to submit a question to all of you for the record about how we—the best tools for trying to get more multilateral cooperation because, of course, the one tool we always have is secondary sanctions, but that is a very blunt instrument. So I am going to pose a question to all of you about how you—how you balance that, when you would use that particular tool.

Thank you.

Chair BROWN. Thank you, Senator Van Hollen. Senator Smith is recognized from her office.

Senator SMITH. Thank you, Chair Brown. Thank you so much to our panelists, and I am glad to be joining you from my office if not in person. So, Ms. Kilcrease, my question is going to be directed to you this morning.

China's military civil fusion strategy, I think, creates some unique obstacles for how to craft and enforce export controls for these dual-use technologies because it is difficult to figure out the technologies intended end uses and end users, and, of course, the rapid pace of innovation and technology only makes this harder. So we need robust controls, export controls that is critical to our national security so that U.S. technologies do not go to unintentionally supporting China's military modernization and intelligence col-

lection efforts. So could you give us your perspective on this? What challenges does China's military civil fusion strategy pose for our export control, and what more should we be doing to address this challenge?

Ms. KILCREASE. Thank you for that question. You know, historically, our export controls try to make distinctions between technology exports that would be for civilian purposes and those that would be used for military purposes. I think we are increasingly realizing that you cannot make those sorts of clear distinctions, and you cannot enforce those distinctions when it comes to the Chinese economy based on the structure of their economy and their clearly stated military civil fusion policies. And so what you have seen in recent years, most notably in the October 7 export controls in 2022 released by the Biden administration, was a response to that, where instead of trying to make these sorts of distinctions, we instead drew a line in the sand, and we said technology that exceeds these technical thresholds is a de facto national security risk if it goes to China, regardless of whether the stated intent is for military purposes or for civilian purposes because we just cannot tell the difference anymore.

And I think that is generally the direction of travel that we need to consider when it comes to technology exports to China. We should not rely on an ability to have full visibility into and be able to enforce in that very difficult context within the China market. I think that certainly applies for the export control conversation. It certainly applies when we are talking about the investment security tools as well. We just have to be very clear-eyed that we are going to have to take these countrywide approaches to imposing controls on these technologies that have such clear relevance for our national security interests.

Senator SMITH. And do you think that step is sufficient, or is there more—what more should we be looking at?

Ms. KILCREASE. I think it is a good start, but that countrywide approach, really, it is limited right now to the controls that we implemented with respect to chips AI in supercomputing. There is a lot more that we can do. There are many more sectors where we should be looking at whether the Control Lists are fully adopting that sort of countrywide approach in some of the sectors that China itself has identified as a priority for them to develop and dominate in the global marketplace moving forward. So we really need to invest and have a keen focus on that continual process of updating the Control Lists, particularly in emerging technology areas, to make sure that they are not stuck in the cold war era but are really keeping peace today.

And then, consistent with the themes we have all been talking about, do we have the analytic capability to understand as we roll out these new and innovative sorts of controls, are they working? Are they slowing Chinese indigenous capabilities in the way that we want them to?

Senator SMITH. Mm-hmm, and thank you for that, and following up on that, and also I think a bit on what Senator Van Hollen was asking about, in addition to sort of taking this approach with our export controls, what more should we be doing to encourage our allies around the world to sort of operate in the same way? I mean,

if we, for example, bar a U.S. firm from exporting technology to China, but they can—you know, they can get the same thing from somebody else, we have not accomplished that much.

Ms. KILCREASE. Exactly. It absolutely needs to be a multilateral approach, and there is a lot more the U.S. could be doing. We currently coordinate controls with key partners under the multilateral export control regime process, but there are some serious questions about whether that is sufficient or fit for purpose. We need to be thinking about how to enhance strategic alignment with our allies, who we do not always agree with, on how to address the China threat, so that is priority number one. Have we convinced them and have we provided the analytic and intelligence argument to our allies to convince them that they also need to be taking this sort of countrywide, broad approach to controls?

And then from there, we need to be going to our partners and allies on a regular basis with a focus on the key producer Nations in these key technology areas and saying, this is what the U.S. thinks we ought to control. Will you come with us? Ultimately, I think ideally what we would like to see is a new export control regime that really allows for a focus on strategic trade controls and the strategic competition with China. There is a lot of skepticism in our key partner countries right now on that idea, so we also need to be thinking about interim steps that we can take to strengthen alignment, but, ultimately, that goal should be a new formalized regime process that really allows us to do this in lock-step with partners and allies on a regular basis.

Senator SMITH. That is great. OK. Thank you so much, Mr. Chair.

Chair BROWN. Thank you, Senator Smith. Senator Warnock of Georgia is recognized.

Senator WARNOCK. Thank you so much, Chair Brown, for this important hearing on our national security and outpacing China.

Last year, the Congress passed the CHIPS and Science Act. It is a piece of legislation I was glad to support and champion. It spurs research in several critical technologies, including quantum computing, AI, cyber infrastructure, and more in our effort to make sure that we remain competitive with China and, in fact, have the competitive edge. Georgia, I am very proud to say, has been leading the country in our efforts to stay globally competitive, using research and development funding from the CHIPS and Science Act to pursue cutting-edge research in healthcare, agriculture, cybersecurity, and beyond.

Chips are in everything, and for the fiscal year 2024, in spite of our passing this legislation in which the Chips and Science Act authorizes over \$26 billion in domestic research investments, and one could make an argument that we should have done more. In fact, the draft appropriations bills only include about three-quarters of that amount. So there is a disconnect between the seriousness of this issue, the importance of us passing that legislation, and where we are right now in terms of appropriations.

Ms. Gorman, as China continues to significantly expand its investments in research and development, do you agree that supporting domestic research is a matter of national security?

Ms. GORMAN. I do, 100 percent, and I think it is one of the top priorities that we should have. The CHIPS and Science Act, which was a historic, bipartisan win, reversed decades of underfunding in our research and development enterprises that have put the United States atop the world, a global leader in many of these exact areas you are talking about: AI, quantum information. We cannot risk having those advantages fall by the wayside, especially when the PRC is moving ahead and trying to become the global leader and outrun us.

These investments are critical, and it should not just be a one-time deal. We have called for a process whereby every year, every 2 years, maybe every 4 years, we reevaluate what are the key technology areas we need to win in the competition, are we resourced for it, and how do we leverage the whole of the American population, all regions, through innovation hubs and tech hubs, toward those goals? This is, I think, almost no higher priority.

Senator WARNOCK. Well, I agree, and the tech hubs is an important provision in that legislation that I have certainly supported. But we hear this argument, or this differentiation between defense and non-defense in terms of appropriations, and if I am hearing you correctly, you would—you would agree that investments in agencies, like the National Science Foundation and the Department of Energy, are critical to our national security, and that the distinction is worse than an academic distinction. It is terribly unhelpful.

Ms. GORMAN. Completely. They are—they are critical to our future competitiveness, which is at the heart of the strategic competition, which is a national security competition with the PRC. We can no longer think only in terms of hard power, especially when the PRC is playing on so many other playing fields. They are weaponizing their economy to coerce businesses to give them technology. They are coercing individuals to silence them on critical issues that the PRC does not want to hear about. This is a full society competition, and so limiting ourselves only to this traditional notion of military hard power misses a huge swath of the competition space.

Senator WARNOCK. Sure. They do not respect these silos in terms of appropriations. Now, in addition to this, it seems to me that we also need researchers and students from all across the country to bring these scientific innovations to life. We need all of our brain power, and that is why I authored a provision in CHIPS and Science to increase research capacity at HBCUs—historically black colleges and universities—and also minority-serving institutions. Supporting these institutions is not simply about equity and diversity. It, too, I would argue, is about national security. If we are going to effectively compete with China, we must find and nurture the finest minds in our country, and as a proud HBCU graduate, I think I know where you can find some of those incredible young people and talent.

Ms. Gorman, what else can Congress do to ensure we are identifying and supporting talent, whether that talent comes from Georgia Tech, Savannah State, or Spelman College?

Ms. GORMAN. I completely agree. We need—this is—this is a tough competition. We need the best and the brightest from everywhere across the country. I think what we—Congress can do going

forward is replicate some of the initiatives that were in the CHIPS and Science Act for other critical technology areas, creating these types of innovation hubs, creating a focus on HBCUs. I saw the Air Force has also partnered with HBCUs in technology development and achievement initiatives like that across these other emerging technology areas, not just the chips manufacturing, which is incredibly important: biomanufacturing, quantum information, agriculture, clean energy technologies. There is so much more we can do, and all our communities are affected, and so we need all of our minds working on the problem.

Senator WARNOCK. Thank you so much. We certainly need to strengthen the pipeline, tap into all of the brain power that we have, and I appreciate your perspective.

Chair BROWN. Thank you, Senator Warnock. Senator Fetterman from Pennsylvania is recognized.

Senator FETTERMAN. Thank you, Mr. Chairman. Thank you, Senator. Thank you, Mr. Chairman. Hi. Thank you. It is great to always talk about the experts, and my first question is to anyone on the panel.

You know, everyone recognizes the danger of IP theft, and China has a well-known history of stealing our intellectual property. Do we agree? Almost, you know, the one copy kind of county. We need to block China from stealing or using our IP to develop and weaponize artificial intelligence. Can anyone on the panel describe the gaps that allow China to steal IP, and how can we cover those gaps?

Mr. JAFFER. Sure. Senator Fetterman, a couple of thoughts. One, you know, the Chinese have engaged in a decades-long effort to steal intellectual property out of American computer systems and the like, millions of dollars a year, billions of dollars in total. General Alexander, the former director of the NSA, called it the greatest transfer of wealth in human history, so we have got to push back. We have got to deter, both at a Government level and an industry level.

Today, private industry is not capable of defending itself. It simply does not have the capacity or knowledge and know-how that the Government has, so we have got to partner tightly between industry and Government. And then second, we have got to really incentivize our cybersecurity defenders and our companies to really protect their own intellectual property. They have every incentive today. We can—we can put more money and more effort into that by giving them tax incentives and the like to better defend their systems.

Senator FETTERMAN. Anyone else on that?

Ms. GORMAN. Yeah. I would—I would just add to that that the problem also exists in terms of forced technology transfers. The allure of the Chinese market remains a compelling factor for companies who want to do business and sell their products in China. Oftentimes it means they are forced to partner with Chinese firms that have an explicit goal of buying them out of the market, taking their technology, and eventually replacing them. I think the short-term capitalism that drives our system is a strategic vulnerability here. We are not necessarily looking to our long-term competitive-

ness when we are so focused on quarterly earnings and quarterly turnovers.

Senator FETTERMAN. I mean, well, this is a hearing, you know, really the title is national security and our challenges in emerging technology. Would you agree with that, that AI would be the single largest, the biggest one, threat or no, or what do you think? Anyone.

Ms. KILCREASE. You know, I think we need to have a holistic approach when we are thinking about the technology competition with China simply because they are as well, right? They are trying to prioritize investments and leadership and domination in a range of sectors. AI, of course, is a really important one. I am just as worried, candidly, about growing market share of China in legacy chip production. That raises a whole host of additional national security risks that we have not even scratched the surface on in terms of appropriate policy responses. So I do think we risk—if we overly focus in one area, we are going to have a blind spot in other areas. So it needs to be biotech, AI, quantum, chips, a whole host of other technologies where China is really making those investments, and we need to as well.

Senator FETTERMAN. I like that. Any others? I really like this—where this is going. Any other—

Ms. GORMAN. Yeah. I would add it is not only the AI threats that were, I think—that are in the popular zeitgeist of these kind of doomsday scenarios and those AI risks. But I would like to see us focus more on, how is China applying AI to all these sectors that they have said that they want to lead in? Those are where we are going to see, I think, the biggest applications of artificial intelligence and the biggest industry and societal advancements. And China is very, very good at taking a technology developed elsewhere and commercializing it and applying it extremely well, and I worry that even though the U.S. has an edge on these frontier models, large language models, once they hit the Chinese market, that they may be able to apply them better than we can. So that is what I would be—one of the things on AI that I am quite worried about.

Mr. JAFFER. I also worry, Senator Fetterman, that we not over-regulate the space, right? If we want to maintain the innovation here in the United States and want to ensure that we continue to lead on frontier models, putting limitations on how those can be utilized and how they might be employed are going to be problematic for further investment and further development of those models. So the right way to approach it, I think, is to encourage and advocate within our industry to ensure that there is trust, safety, and security baked into our models, that we are auditing them, that we are thinking about how they are being utilized, that we are deploying them and testing them before we put them out in the world.

At the same time, artificially limiting them by, you know, measuring how many—how many—how much computing power they use or how many—how many elements they process, I think, could be a mistake and allow China to get the edge. We do not want to allow that to happen. We want to make sure that investment and that capability stays here in the United States. And then we also

need to be cognizant of how much data China is acquiring and how they use that data to empower their ability to repress their own people and to act against the United States.

So when we look at capabilities like TikTok, people say, why worry about cat videos? Exactly. It is not just cat videos. It is data about average Americans. The idea that TikTok buys ads at DCA and is convincing Americans and American legislators through those ads is outrageous. The Metropolitan Washington Airport Authority ought to be embarrassed that they are—that they are having ads at Union Station and at DCA for TikTok, a Chinese Government influenced—media influence operation.

Senator FETTERMAN. I wish I had an hour because you guys all touched on really critical kinds of issues and where this can go or what is possible, but I know we have—unfortunately, we have lost our time, but back to you, Mr. Chairman.

Chair BROWN. Thank you, Senator.

Senator FETTERMAN. And thank you for the experts.

Chair BROWN. Senator Fetterman, thank you. I know you almost always go last, but thank you for always your thoughtful questions and response. Thank you to the three witnesses, a really, really good hearing, and thank you so much for that.

For senators who wish to submit questions for the record, those questions are due 1 week from today, January 25, please. To the witnesses, you have 45 days, if you would, to respond to those questions. Thank you again. With that, the hearing is adjourned.

[Whereupon, at 12:05 p.m., the hearing was adjourned.]

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

PREPARED STATEMENT OF CHAIR SHERROD BROWN

Last week, this Committee heard about the human toll that illicit fentanyl takes on our families, our friends, our neighbors.

The witnesses stressed the need to come together and taking action to stop the flow of illicit fentanyl from China and Mexico.

This Committee and the entire Senate did just that last year when we included the FEND Off Fentanyl Act in the annual defense authorization bill. But this hasn't become law yet, because of politicians in the House playing politics.

The FEND Off Fentanyl Act was not the only Committee priority that the House blocked last year.

They also blocked two other important national security amendments in the Senate NDAA—both of which received 91 votes in the Senate.

Ninety-one senators voted in favor of an amendment offered by our colleagues Senators Tester and Rounds to prevent big investors in China from buying up American farmland and food businesses. We can't allow foreign adversaries to buy up farmland in Ohio and around the country. It's a threat to our national security, and it's a threat to rural economies and our way of life.

Ninety-one senators also voted in favor of an amendment offered by Senators Casey and Cornyn to allow us to better monitor U.S. companies' investments that fund Chinese development of critical technology, including military technology.

All three of these provisions have broad support—from Heritage Action to the Coalition for a Prosperous America.

And more importantly, they have the support of the public. For far too long, our policy around China catered to multinational corporations, and failed States like Ohio. On this Committee we are working to change that, and we have found common ground. It's why all three of these bills remain top priorities of this Committee.

I am committed to working with my colleagues to find a path forward so that each of these provisions becomes law this year.

Of course the threats posed by China are many, and varied, and growing. Our work to address national security risks posed by the Chinese Government cannot and will not end with those three provisions.

We all agree that China poses a real and growing threat to our national security.

Perhaps nowhere is that risk more acute than with the development of advanced technology.

China has used advanced technology—much of it stolen from the U.S., some of it sent there through corporate outsourcing—to ramp up its military modernization and build a mass surveillance State that commits deplorable human rights violations, including the detention of millions of Uighurs in Xinjiang.

Addressing these threats from the Chinese Government, and improving our domestic capability to compete with China, have been a top priority of this Committee.

Five years ago, we updated the laws that govern our export control and inbound investment screening programs.

Now we must assess whether our current authorities—and the resources we commit to them—match the threat we face.

Export controls can be used to deny China and others access to U.S. technology that they could use against our national security and foreign policy interests.

This Administration has made export controls a central feature of our national security policy.

In addition to assembling a global export control coalition in response to Russia's war against Ukraine, this Administration has added hundreds of China-based entities to restricted trade lists. It imposed countrywide controls that restrict China's access to advanced semiconductors and tools and equipment needed to produce them. And it ramped up enforcement efforts to safeguard our most sensitive technologies.

But, as Commerce Secretary Gina Raimondo noted in December, the export control budget of the Bureau of Industry and Security is roughly the same as it was a decade ago, despite its increasing workload.

If we agree that export controls are critical to our national security, and I think we do, then that isn't good enough.

We need a China policy for the world we live in today, and we must prepare for what could come tomorrow.

That means we must upgrade our economic security authorities and resources, accelerate efforts to persuade other countries to join us, and enhance our analytical capabilities, so that we can better understand the effects that our economic security tools have on China, on U.S. companies, and on companies in partner countries.

Today we will discuss how we should rethink and reorient how economic security programs are implemented to address the full range of risks posed by China.

And we will examine how we can strengthen these authorities and resources to build a stronger, more responsive economic security policy.

Our country's policies regarding China have failed for too long. They've been written to increase the profits of multinational corporations looking for cheap labor—not to benefit our national security, and not to benefit American workers.

And we know that when companies outsource jobs, they outsource innovation and technological capabilities along with them. We cannot allow China to continue to use that technology—in many cases, steal it—to enhance its military capabilities.

We all agree that China is a real, growing threat.

Countering that threat, and updating the failed policies of the past, will continue to be a bipartisan focus of this Committee.

PREPARED STATEMENT OF SENATOR TIM SCOTT

Thank you, Mr. Chairman. Good morning to the witnesses, thank you for being here as well. Thank you Mr. Chairman for this opportunity to talk about such an important topic.

But before turning to this hearing, I'd like to take a moment and draw attention to the recent Iran-backed strikes in Iraq.

Any time American lives are put at risk, whether it's from Iran or their terror proxies like Hamas, we need to have a strong response. And that starts with this chamber passing my Revoke Iranian Funding Act.

Every dollar that goes to Iran from this Administration's actions, is a dollar that supports terror. Thank you.

America is the land of opportunity and freedom, the opportunity to innovate, produce, and execute on individual ideas.

These principles are what drives our strides in technological innovation, and our emphasis on entrepreneurship.

We have the strongest economy in the world, driven by its dynamic growth and evolution. We are the global gold standard that countries look on with envy.

However, American exceptionalism is under attack from a country that doesn't want to play by the rules—that country is obviously China.

To make sure our success does not become the victory of others, the United States Government must act strategically and with strength, in protecting opportunities for growth at home and abroad.

When we look at adversaries like the Chinese Communist Party with their centrally planned economy that actively works to distort global markets for its own gain and continuously makes overt attempts to oust us from our perch of leadership.

We don't have to ask the question—are they playing by the rules?

Because we already know the answer to the question, and the answer is emphatically no.

But China's approach—with their controlled markets, Government interventions, and intellectual property theft—is shackled to the openness of others.

So, we must act strategically to ensure that we are safeguarding America's treasure—our ability to innovate.

We cannot let China continue its malign activities, especially in regards to using, or even stealing, American innovation and American technologies for nefarious purposes, like advancing its rapidly growing military.

So, as we consider American security and prosperity from the Banking Committee's jurisdiction, we should look first at our economic security tools.

We need to examine the authorities provided to the executive branch, how they have been used, and how they can be improved for maximize effectiveness.

However, an over-application of these tools has the potential to push our adversaries closer together and damage the U.S. and our industries' long-term abilities to innovate and generate jobs and to generate growth.

Therefore, our use of these tools must be sharp but tailored.

Thankfully, we can isolate bad actors through our sanctions policies, we can restrict malign investment through our CFIUS process, and we can curtail the export of critical goods and services to our enemies.

These actions are stronger when we work together with our allies and stay focused on the true problem at hand.

But unfortunately, this Administration is yet again, taking the wrong approach.

This Administration has put politics over policy, and in some ways, that is playing right into the hands of China.

For example, the Department of Commerce's Bureau of Industry and Security, the steward of our export controls, is currently engaging in politically motivated attacks against the legal firearms industry.

A troubling trend by this Administration's regulators to try to target lawful businesses through the regulatory process that don't fit their political narrative.

This undercuts the Commerce Department's important mission of safeguarding U.S. technology, opening the door for distractions that will allow the CCP to take advantage.

But Commerce isn't the only perpetrator.

The Department of Treasury's primary focus appears to be on pursuing the limits of climate and green energy financing policy.

And frankly, these objectives only advance China's solar and critical mineral energy positions in geopolitical affairs.

Treasury's time, attention, and taxpayer-provided resources would be much better spent working to ensure our sanctions policies on China remain up to date and promoting as well as protecting American industry abroad.

We need an Administration that is focused on countering the real threat—China—not one that is more interesting to politics.

So, while I am grateful that we have such an esteemed panel before us today, I think it is imperative we hear directly from the Administration as well.

That said, I look forward to hearing from each of you, and your expertise on the issues that will help strengthen our economy, and strengthen our position against China.

And, importantly, to learning more from their perspectives on how we should act and respond to the threat.

PREPARED STATEMENT OF EMILY KILCREASE
SENIOR FELLOW AND DIRECTOR OF THE ENERGY, ECONOMICS, AND SECURITY
PROGRAM, CENTER FOR A NEW AMERICAN SECURITY
JANUARY 18, 2024

U.S. Economic Security Strategy, Authorities, and Bureaucratic Capacity

January 18, 2024

I. Summary of Testimony

Chairman Brown, Ranking Member Scott, and Members of the U.S. Senate Committee on Banking, Housing, and Urban Affairs, thank you for the opportunity to provide testimony. While I am currently employed by the Center for a New American Security (CNAS), I am providing testimony in my personal capacity.¹ The testimony draws from a large body of research that I have conducted at CNAS, as well as my prior experience serving the U.S. public as a proud civil servant in the U.S. Department of Commerce, the National Security Council, and the Office of the U.S. Trade Representative, including most recently serving as the Deputy Assistant U.S. Trade Representative for Investment.

At the request of the Committee, this testimony focuses on three economic security tools that the United States has or is considering establishing: export controls; screening of inbound foreign direct investment (FDI), as implemented by the Committee on Foreign Investment in the United States (CFIUS); and the possibility of new authorities related to outbound investment controls. Specific analysis and recommendations for enhancing the capacity and effectiveness of each of these economic security tools is included, with a focus on how these tools can be used to maintain a U.S. technological lead vis-à-vis China. The testimony focuses on issues of strengthening economic security strategy, authorities, and bureaucratic capacity, rather than advising on specific technologies that may be suitable for more or fewer controls. Given common issues across the programs and the acute need for stronger integration and coherence across the economic security toolkit, the testimony begins with cross-cutting recommendations.

A summary of recommendations for congressional consideration are as follows:

Cross-cutting issues in the economic security toolkit

- Direct the administration to develop an economic security strategy that defines a clear vision for bounding the economic relationship with China to address national security risks, including specific and measurable plans for the use of economic security programs to address national security risks;
- Establish and provide resources for strategic planning functions in the agencies responsible for managing economic security programs, including dedicated full-time staff for strategic planning;
- Promote stronger alignment on economic security with key international partners and allies, including through guidance on the types of formal or informal arrangements that can facilitate stronger collaboration and resources to support expanded international outreach efforts;
- Establish and provide resources for dedicated offices to evaluate the effectiveness of existing and proposed economic security policies; and
- Facilitate government access to diverse, unbiased sources of information and expertise, including from industry, the intelligence community, and independent analysts.

¹ This testimony reflects the personal views of the author alone. As a research and policy institution committed to the highest standards of organizational, intellectual, and personal integrity, the Center for a New American Security (CNAS) maintains strict intellectual independence and sole editorial direction and control over its ideas, projects, publications, events, and other research activities. CNAS does not take institutional positions on policy issues and the content of CNAS publications reflects the views of their authors alone. In keeping with its mission and values, CNAS does not engage in lobbying activity and complies fully with all applicable federal, state, and local laws. CNAS will not engage in any representational activities or advocacy on behalf of any entities or interests and, to the extent that the Center accepts funding from non-U.S. sources, its activities will be limited to bona fide scholarly, academic, and research-related activities, consistent with applicable federal law. The Center publicly acknowledges on its website annually all [donors](https://www.cnas.org/about/funding) who contribute.

Export controls

- Increase the budget for the Bureau of Industry and Security to match its expanded national security and foreign policy mandate and to enable it to fulfill new responsibilities related to strategic planning, evaluation, and international outreach;
- Mandate regular reviews of the Commerce Control List;
- Assess the effectiveness of country-wide controls on commercial technology exports to China, including the impacts on U.S. competitiveness and the feasibility of securing support for such controls from key international partners;
- Mandate the evaluation of novel export controls, such as the foreign direct product rules; and
- Require a study on the feasibility of releasing additional export control data to the public.

Committee on Foreign Investment in the United States (CFIUS)

- Expand the CFIUS definition of “critical technologies” to include “critical technologies controlled for investment purposes,” as defined by CFIUS and focused on emerging technologies; and
- Address high case volumes and potential mission creep by passing data security and data privacy legislation and conducting oversight on the use of mitigation agreements for transactions involving firms located in U.S. allied countries.

Outbound investment controls

- Codify and provide resources for a targeted set of outbound investment controls focused on transactions that may enable China’s indigenous development of technologies relevant to U.S. national security interests;
- Require mandatory notifications of U.S. investments in China to enhance U.S. government insights into the scoping and administration of outbound investment controls;
- Prohibit U.S. investments into high-risk technologies or sectors in China; and
- Expand the Non-SDN Chinese Military-Industrial Complex program to prohibit all types of investments in listed entities.

II. Introduction

China is a foremost geopolitical challenge for the United States. As Secretary of State Anthony Blinken has stated “China is the only country with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to do it.”²¹ Unlike prior eras of strategic competition, China is deeply integrated with the U.S. and global economies, creating new types of national security risks from China’s potential to weaponize these economic ties. While strategists might have previously bet on economic entanglement leading to geopolitical stability, Russia’s brutal invasion of Ukraine and the increasingly authoritarian bent of China under Xi Jinping have rightly shaken policymakers’ reliance on this view. The urgent task for the United States now is to mitigate national security risks arising from the



economic relationship with China, prevent China from exploiting the open nature of the U.S. market, and anticipate future risks that may emerge due to the rapid, global advance of critical technologies.

Meeting the China challenge will require the U.S. government to prioritize economic security programs (i.e., programs that address the national security risks that can arise from economic activities), including expanding the legal authorities and resources available to these programs across the executive branch. In the post 9/11 period, the Department of the Treasury was transformed to address the threat of terrorism, leading to major changes in how the United States can target the illicit sources of finance.² The U.S. government is in a similar moment now, with the need to fundamentally rethink and reorient how economic security programs are implemented to address the full range of risks presented by China. Technology competition is at the core of the U.S.-China strategic competition, and the role of technologies in economic security should be central to a strengthened government capacity to counter the China challenge.

III. Cross-cutting Issues in the Economic Security Toolkit

Too often, economic security issues are dealt with in bureaucratic silos. Economic security strategy tends to be a greatest hits list of what the government is already doing and has always done, rather than setting an ambitious vision to guide the use of economic statecraft tools. Program implementers stay confined to their area of bureaucratic turf and, through no fault of their own, are often too consumed by the intense day-to-day demands of dealing with ongoing crises to advance longer term objectives. These dynamics do not bode well for the whole-of-government approach needed to transform the U.S.-China economic relationship to better serve U.S. strategic interests and advance democratic values.

Congress can act to remedy these negative dynamics, including through directing the executive branch to develop an economic security strategy; establishing and providing resources for strategic planning functions in the economic agencies, including through dedicated full-time staff; pushing for greater alignment of U.S. economic security strategies and policies with key international partners; strengthening the government's capacity to evaluate the effectiveness of economic security programs; and ensuring that economic security functions have access to a wide range of non-biased, technical information.

U.S. Economic Security Strategy

The United States needs an economic security strategy. The Department of Defense recently released a defense industrial base strategy, the Department of Commerce is reportedly set to release its own national security strategy, and the Department of the Treasury in 2021 released a sanctions strategy.³ That each agency is developing and releasing its own strategies is emblematic of the larger problem: the United States does not have a holistic vision for how to utilize all of its economic tools in tandem to achieve an articulated end state in the economic and geopolitical relationship with China.⁴

Recent CNAS research put forth one framework for developing economic security strategies, including introduction of the concepts of economic domain ends, ways, and means:

- **"Ends** specify the desired end state between the U.S. economy, its partners' economies, and that of its adversary, and are derived from broader ... strategic objectives....
- **Ways** are the various methods of applying economic pressure ... including a range of coercive economic statecraft measures such as financial sanctions, technology export controls, and tariffs.
- **Means** are defined in terms of the United States' relative capacity in an area of strategic economic activity."⁵

While this economic domain ends, ways, and means construct was developed in the context of research on sanctioning China in the event of a conflict, it equally applies to managing the economic security relationship



today. The United States must set a clear vision for what a future economic relationship with China looks like, balancing the economic need for continued ties with the security need to de-risk certain areas of economic activity. This vision should be derived from the broader national security strategy and focus on addressing the risks to national security that can arise from economic activities.⁶ It then needs to develop specific, measurable strategies for how it can use all tools of economic statecraft to achieve the desired end state. Statements from administration officials have planted the seeds for what a potential strategy could look like, but none yet provide a clear view on how the United States should define the economic relationship with China to address growing national security concerns.⁷ This is a particularly important gap, as the range of sectors that are assessed to have national security implications continues to grow and now encompasses much broader swathes of ordinary commercial activity.

This testimony focuses on three areas within the economic security toolkit. However, the potential range of policies and programs that could be used to advance U.S. economic security objectives (i.e., economic domain ways) are much broader and include tools such as tariffs and trade policy, subsidies, and restrictions on the import of information technology goods and services. Government procurement can also be used to address economic security issues, and Congress is considering bipartisan legislation to address government contracting with Chinese biotechnology companies, in one example of where this may be relevant.⁸ How these tools are used in tandem to promote U.S. technological leadership should be a core element of an economic security strategy.

Semiconductors can provide a useful case study in the need for more holistic strategies. The United States has taken proactive steps to maintain U.S. advantage in advanced chips, including through precedent-setting export controls on technologies China needs to make advanced chips, as well as a large push on industrial policy to support domestic chips production and research and development. So far, so good. However, the effect of these policies is to create a structural incentive for China to double down on investments in legacy chip production, and the United States is not prepared to address a surge in imports of Chinese legacy chips.⁹ Export controls would likely be ineffective, simply because China already has the technology necessary to make such chips. Tariffs, import restrictions, government procurement policies, and outbound investment controls could all play a role in addressing the import problem, though whether they can slow China's global growth without harming U.S. economic interests remains unclear. A more deliberative process for setting economic security strategy should anticipate these sorts of unintended consequences to enable more nimble and effective U.S. response to shifting market dynamics, including those shifts that are caused by actions of the U.S. government itself.

An effective economic security strategy will require breaking down of bureaucratic siloes and a sharp focus on prioritization of issues. It will require working across all the economic agencies in the executive branch and across multiple committees of jurisdiction in Congress. As officials proceed with developing economic security strategy, they must remain laser focused on addressing the most pronounced gaps in the U.S. toolkit. In addition to continual updating of export controls and CFIUS, passing legislation to address problematic vacuums in U.S. authorities, such as those related to outbound investment and data security (discussed further in later sections of the testimony), are an important part of an effective economic security strategy.

Strategic Planning Functions¹⁰

The agencies responsible for managing economic security programs should establish strategic planning functions, which would continually assess how economic security tools could effectively be used in a range of potential future scenarios with strategic competitors, with a focus on China. While this sort of strategic planning function is well established in the military community, it is practically non-existent for the economic agencies. Yet, should a crisis or conflict with China break out, economic tools would almost certainly be part of the U.S. policy response. An economic domain strategic planning process can enhance U.S. readiness for



such scenarios, as well as enable the United State to consider the deployment of economic tools in support of longer-term deterrence objectives and in the ongoing strategic competition with China.

Economic domain strategic planning should be carried out at three levels.¹¹ First, the economic agencies must deepen their institutional capacity to engage in long-term strategic planning. Second, planning must be integrated with similar planning exercises in the defense community in support of an “integrated deterrence” objective that utilizes all instruments of national power.¹² Third, U.S. planning must be integrated with that of U.S. partners and allies, leveraging the core U.S. strategic advantage of alliances.¹³ Each of these areas must be staffed by experts whose full-time job is strategic planning, to avoid falling into the familiar trap of pushing off long-term thinking in order to deal with the crisis of the day.

Alignment with International Partners and Allies

Economic security programs are maximally effective when the U.S. approach is aligned with that of its key allies and partners abroad. While unilateral controls may be effective in the short-term and in some cases may be necessary to spur action from partners and allies, the effectiveness of unilateral measures erodes over time. U.S. firms must vigorously compete to maintain their leading role in global technology value chains, and restrictions only on U.S. firms will ultimately lead to foreign firms backfilling U.S. technology exports to China.¹⁴ A classic case in this regard is U.S. export controls on satellite technology. Europe did not implement similar controls and European firms were active in advancing China’s satellite technology developments.¹⁵ In these scenarios, the United States has the worst of both worlds—lost revenue and minimal impact on China’s indigenous technology development.

Various experts have put forth proposals for structures to enhance alignment on economic security with international partners. A new multilateral export control regime, designed with strategic trade control objectives in mind, could complement the current Wassenaar Arrangement structure, which coordinates country-agnostic controls.¹⁶ Broader agreements could be negotiated with partners that enhance coordination on a range of economic security tools, including export controls and investment security but also encompassing supply chain resiliency tools.¹⁷ Or, efforts could focus on strengthening the ability of partners and allies to implement unilateral controls under their domestic authorities, providing needed flexibility when the United States seeks to form ad hoc coalitions, such as it did recently with the Netherlands and Japan on semiconductor manufacturing equipment export controls. Ultimately, the right approach will be the one that can secure broad buy-in from a range of industrialized and emerging economies. To date, key partners have expressed skepticism about the viability of new formalized regimes, though multiple efforts at strengthening cooperation are underway (e.g., coordination on export controls and investment screening in the U.S.-EU Trade and Technology Council).¹⁸

To meaningfully advance international alignment, the United States must work with allies to address divergences in their strategic assessments of the threat presented by China, their legal frameworks to impose new controls, and their capacity to implement and enforce more robust economic security programs. Some progress has been made in strategic-level alignment, including at the G7, which issued an important leaders’ statement on economic security and resiliency this past year.¹⁹ While the views of many partners toward China are hardening, not least because of China’s continued support of Russia’s invasion of Ukraine, there remain important differences in their views on how hard and fast to pursue economic de-risking with China.²⁰ Divergent views on the threat posed by China will necessarily complicate efforts to align the development and use of economic security tools to address this threat.

U.S. partners and allies also tend not to have the same broad and flexible economic security programs that the United States enjoys. On export controls, the legal authorities of most partners and allies are limited to implementing the export controls agreed in the multilateral export control regime processes and they do not have easily available ways to impose unilateral controls.²¹ FDI screening mechanisms vary, and while many



countries now have such mechanisms, their legal scope and maturity vary considerably. Very few partners and allies have outbound investment screening, with most U.S. partners and allies expressing some skepticism about the need for such authorities and waiting for the United States to act first before deciding whether to implement their own outbound investment programs. Further, international capacity to implement economic security programs lags that of the United States, with partners and allies tending to have smaller staff and more limited intelligence capabilities. These dynamics mean that the United States must prioritize outreach and technical assistance to partners and allies, as U.S. support and leadership can play a critical role in strengthening the economic security efforts of U.S. partners and allies.

Congress could promote stronger international alignment by pushing the administration to prioritize economic security issues in its diplomatic efforts with international partners, including important technology players in Europe and Asia. It can provide clear guidance on the types of formal institutions or agreements that the United States should seek to establish, while also setting realistic interim goals on strengthening alignment while such institutions or agreements are being considered by international partners. Funding the international coordination functions of the economic security agencies will be critical, as well as ensuring that the State Department political and economic officers have training in economic security issues and a mandate to prioritize U.S. economic security objectives in their engagements with foreign counterparts.

Evaluation

Economic security tools are being used at an unprecedented scale and for a range of novel policy purposes. Export controls, for example, have evolved from a limited tool designed to prevent accumulation of weapons into one of the United States' favored policy responses to address a broad range of national security and foreign policy objectives.²² While the use of economic security tools is justified on national security grounds, policymakers must not forget that imposition of economic restrictions come with economic costs. Economic restrictions, if effective, shut off market access to one of the world's most consequential economies, which has for decades been a driver of scale and growth for U.S. technology companies. As the range of economic security policies continues to grow, the U.S. government must have a way to assess the cost and effectiveness of these measures, including their long-term impact on U.S. technological competitiveness.

Currently, the evaluation function for economic security policies is sorely under-resourced. While the Department of the Treasury has established an office to assess the economic impacts of its sanctions programs, no comparable office exists for other economic security tools. Congress could consider establishing new offices within the Departments of Commerce and the Treasury to evaluate the effectiveness of export controls and investment security programs, while also assessing the impact of these programs on overall U.S. competitiveness. The evaluation of these offices should be used to inform the development of new economic security measures and the updating of existing ones. In cases where a measure may have high cost but is necessary nonetheless for national security reasons, these evaluations can inform how the government might use other policy tools to mitigate any impacts on U.S. competitiveness.

Access to Information and Expertise

Effective implementation of economic security programs depends on access to diverse, unbiased sources of information and expertise. These programs must have deep knowledge in legal and regulatory issues, market issues, critical technologies, China's economic and technology landscape, and U.S. technological capabilities. Specialized skills, such as Mandarin language skills or deep technological expertise, are often in short supply within the government. While the agencies should prioritize hiring staff who possess these types of expertise, in reality the scope of expertise needed will always outpace the government's ability to hire, particularly when considering the fast pace of technological development in the commercial space. The economic agencies will need to leverage a wide range of sources of information and expertise, including:



- **Industry:** Industry often has the most up-to-date and detailed information on technology products, simply because it is their engineers who develop these products. Regular engagement with industry can help government policies keep pace with commercial developments, while also alerting the government to unintended consequences of specific policies. At the same time, an over-reliance on industry sources should be avoided, as industry will have an inherent bias in its perspective.
- **Intelligence:** The intelligence community must provide robust support to economic security functions. Ways of achieving this vary. In the CFIUS process, the Office of the Director of National Intelligence (ODNI) provides coordinated intelligence assessments for each transaction under review. For sanctions, Treasury has its own intelligence capabilities through TFI. For export controls, Commerce has an analytic office that provides support for enforcement purposes.
- **Independent analysts:** Independent, third-party organizations, such as think tanks, federally funded research and development centers, academia, and business intelligence services, can also act as sources of unbiased technical and strategic information for economic security programs.²³

Congress could utilize its oversight functions to ensure that the economic security agencies are fully utilizing these sources of information. While not endorsing any particular proposal for ensuring more robust intelligence support for the export control programs, Congress could focus on whether the growing national security role of the Department of Commerce has sufficient support from the intelligence community. This should include intelligence support for export control licensing decisions and development of new export control policies, in addition to intelligence support for enforcement efforts, and should include capabilities to conduct Chinese-language, all-source intelligence analysis. Congress might also consider whether the agencies have sufficient resources to subscribe to business intelligence platforms or commission third-party studies, if doing so would support their overall missions.

IV. Export Controls

Export controls regulate the export, re-export, and in-country transfer of commodities, software, technologies, and, occasionally, services to specific destinations, end users, and end uses to achieve U.S. national security and foreign policy objectives.²⁴ The classic post-Cold War objectives of export controls were to regulate bespoke military and dual-use items (i.e., items with both military and commercial applications) that had some identifiable relationship to the development, production, or use of either weapons of mass destruction or conventional weapons.²⁵ With the export controls imposed against Russia in early 2022 and against China in late 2022, the U.S. government has expanded the scope of export controls to address broader strategic objectives regarding otherwise exclusively commercial items that nonetheless are of importance to the industrial bases of Russia and China.²⁶

Dual-use export controls, which are the subject of this testimony, are governed by the Export Control Reform Act of 2018 (ECRA). ECRA provides broad authority for the United States to impose unilateral or multilateral controls to address a range of national security and foreign policy objectives, including those related to combatting weapons proliferation and terrorism, preserving the military superiority of the United States, strengthening the U.S. defense industrial base, protecting human rights and democracy, and facilitating military interoperability with allies.²⁷ Dual-use export controls are administered by the Department of Commerce, in close coordination with the Departments of Defense, Energy, and State.²⁸

While Commerce and the export control agencies have a strong legal framework to implement controls for a broad range of national security and foreign policy objectives, their ability to do so may be hampered by under-resourcing, as well as a current lack of capacity to regularly evaluate the effectiveness of existing and proposed controls. The issues of resourcing and evaluation are further stressed by the greater role that export



controls are playing in U.S. national security and foreign policy, including the implementation of new and innovative types of export controls, the long-term effectiveness of which has not yet been proven.

Resources for an Expanded National Security and Foreign Policy Mandate

Export controls now play a leading role in U.S. foreign policy, not just in the China context but also as part of the sanctioning effort toward Russia and bolstering human rights, among other objectives.²⁹ As new and continually more novel types of export controls continue to be implemented, there is an acute need to ensure that Commerce has the corresponding increase in resources to monitor and enforce its new controls. Secretary of Commerce Gina Raimondo has urged Congress to invest in export controls, stating that the Bureau of Industry and Security (BIS), the agency within Commerce that administers export controls, has the same budget it did a decade ago (that is, before the Russian invasion of Ukraine and before the rise of Xi Jinping).³⁰ As one export control official noted, “[w]e spend 100 percent of our time on Russia sanctions, another 100 percent on China and the other 100 percent on everything else.”³¹

Examining the budget numbers for BIS provides another perspective on the question of resources. BIS’s enacted budget in 2012 was \$101 million (adjusted for inflation, this number would be approximately \$133 million).³² In 2023, the enacted budget was \$191 million and the requested budget for 2024 is \$222 million.³³ However, while resources may appear to be growing for BIS, a substantial portion of these increases have been driven by non-export control related activities, such as the implementation of new authorities related to regulating the imports of information and technology goods and services, as well as adjustments for inflation and mandated civilian pay increases.³⁴ This suggests that resources for the functions described in this testimony (strategy development, strategic planning with the interagency and international partners, evaluation of existing and proposed controls) remain a gap that Congress may want to address through further investment in BIS capacity in these areas. To date, these functions either do not exist or are under-resourced relative to the national security need. Additionally, established functions in export administration and export enforcement are likely not receiving sufficient investment, given growing demands. For example, the number of licensing applications has grown on average in recent years, with applications peaking near 40,000 in 2020 compared to annual averages closer to 24,000–31,000 in the 2014–2015 period.³⁵ Increased use of extraterritorial controls, discussed in more detail later, also increases the need for export control officers to be based overseas to conduct monitoring and enforcement activities.

Think tank analysis has proposed increased funding levels for particular BIS programs. CNAS AI researchers recommend \$10 – 12 million in funding to implement an AI chip registry and random sampling program, both of which are intended to bolster technical methods of export controls enforcement.³⁶ The Center for Strategic and International Studies recommends approximately \$45 million to modernize analytic and enforcement capabilities.³⁷ Importantly, these analyses recommend not just more money, but more money wisely spent. The fast-expanding scope of export controls and complex enforcement environments mean that simply scaling up existing processes are likely to be ineffective. Innovative technical approaches to enforcement, such as using on-chip governance mechanisms to track the deployment of advanced AI chips, should be part of Congress’s considerations related to increased resources.³⁸

Many recommendations in this testimony, including the review of the Commerce Control List, establishment of strategic planning and evaluation functions, international engagement, and public release of export control data, would all require resources, which Congress should assess.

Regular Review of the Commerce Control List

As the United States continues to expand the national security and foreign policy objectives for which it uses dual-use export controls, it must regularly review its control lists to ensure that it is capturing those technologies relevant for these expanded objectives. The Commerce Control List is the vehicle for listing and



controlling dual-use technologies, including the licensing policies for each listed technology.³⁹ It is questionable whether the Commerce Control List is reflective of today's high-priority, national security-relevant technologies, particularly with respect to emerging technologies. Regular and holistic reviews of the Commerce Control List could help ensure that it reflects the current state of technological competition with China, including in emerging technology areas that currently do not have high levels of controls (e.g., AI).

Congress could direct—and provide resources for—Commerce to conduct a top-to-bottom review of the Commerce Control List, report to Congress on the results, and provide a plan for updating controls based on this review within a set period. The review could include all items currently listed for any reason on the Commerce Control List, as well as examination of whether new controls should be implemented for those technologies that were identified in the list of critical and emerging technologies developed by the White House Office of Science and Technology Policy and the National Science and Technology Council.⁴⁰ Recent requirements to review the U.S. Munitions List can inform additional aspects of the suggested Commerce Control List review, including that it should consider interagency resources to implement existing and future controls, evolving technological and economic factors, and whether such technologies are available from other suppliers globally.⁴¹ Congress could consider requiring regular reviews to ensure that there is continued attention and prioritization of list updates to keep pace with changes in the threat and technology landscapes.

Related to points made in the cross-cutting analysis of this testimony, reviewing the Commerce Control List will require Commerce to have access to a wide range of unbiased technical expertise. While Commerce should work companies to benefit from their technical and commercial knowledge, an industry-heavy approach to updating the Commerce Control List will be insufficient to meet current U.S. national security needs. Commerce will need to leverage expertise from other sources, including close coordination with the Departments of Defense, State, and Energy, as well as the intelligence community. Congress could require such interagency coordination and intelligence support as part of its direction to Commerce to conduct the list review. Additionally, Congress could consider specific funding for external analysts to conduct research in support of the list review. Regardless of the source of expertise, certain skills will be critical: Chinese language capabilities, industry and markets expertise, trade data analysis, engineering and technical knowhow, and expertise in China's indigenous technology development capabilities.

Country-Wide Controls in Response to Military-Civil Fusion

The United States has begun to implement country-wide controls on certain technologies in response to China's military-civil fusion strategies. Dual-use export controls have historically been implemented to prevent the flow of sensitive goods to military end uses or users while permitting the flow of goods to commercial purposes. However, China's military-civil fusion strategy complicates efforts to make clear distinctions between what is commercial and what is military. The merging of the civilian and military spheres is seen as a critical way by which China can leverage the whole of its economy in support of its military modernization goals, including through the development or acquisition of dual-use technologies such as semiconductors, AI, and quantum computing.⁴²

The October 7 export controls on chips, AI, and supercomputing reflect a new U.S. approach for responding to China's military-civil fusion. These controls do not attempt to distinguish between military and commercial purposes. Instead, they establish a bright line test to prohibit the export of certain technologies to China based on how advanced a technology is and are applied for *all* users and purposes in China. The stark implication of this approach is to declare the further advancement of China in these technology areas to be a de facto national security risk, regardless of whether the advances are used for civilian or military purposes. As National Security Advisor Jake Sullivan noted, the new U.S. objective is to use export controls to maintain "as large a lead as possible" over China in those technology areas that are "force multipliers" for U.S. technological leadership.⁴³



Congress has an important role to play in assessing whether this country-wide approach to controlling exports of dual-use technologies is effective. To date, certain October 7 controls have been complemented by similar controls from U.S. partners, namely controls on advanced semiconductor manufacturing equipment that were implemented by the Dutch and Japanese governments. However, many partners are skeptical of the new U.S. approach, and Congress should push the administration to prioritize further alignment on country-wide controls with key international partners. As with all controls, a more aggressive strategy of using country-wide controls will likely be unsustainable over time if not supported by like actions from other key producer nations.

Congress could push the administration to provide additional clarity and guidance on which sectors are suitable for country-wide controls. To date, semiconductors have been the focus of this approach, but the administration appears to be considering new controls in other areas, including cloud computing and quantum technologies.⁴⁴ International partners will need this type of clarity to understand the full breath of the administration's strategy, and additional assurances that the strategy will remain contained to a "small yard, high fence" philosophy, as the administration currently claims, will likely be necessary to secure their support for any future controls.⁴⁵

Congress could encourage a consistent approach to using country-wide controls across the economic security tools. For example, the administration's executive order on outbound investment includes a prohibition on U.S. investments in Chinese companies involved "in the development of software that incorporates an AI system and is designed to be exclusively used for military, government intelligence, or mass-surveillance ends uses."⁴⁶ This very narrow scoping is unlikely to cover many AI systems, given that few if any AI systems are "exclusively used" for purely military ends. This type of measure, which will likely return a null set, appears to be inconsistent with a strategy designed to apply economy-wide controls on force multiplier technologies such as AI.

Evaluation of Novel Export Controls

While strengthening government capacity to assess the effectiveness of all export controls is essential, it is particularly critical to evaluate the use of novel export controls that are now being used in unprecedented ways, including to achieve new types of national security and foreign policy objectives. Foremost among these are the foreign direct product rules (FDPRs).

FDPRs are an oft-cited and oft-misunderstood tool. An FDPR allows the U.S. government to apply a control to a foreign-made product, if that foreign-made product is manufactured using U.S. technologies. U.S. technology need not be integrated into the foreign-made product for the FDPR to apply (controls related to integration of U.S. technology into a final good are addressed under a separate set of *de minimis* rules). Instead, the regulatory hook could simply be that a U.S. machine was made to manufacture a foreign good, even if that foreign good has absolutely no U.S. content integrated into it. The foreign-made item is subject to the export control so long as the foreign manufacturer continues to use the U.S. machine to produce its products. Each application of an FDPR is bespoke and designed for a specific scope of products and technologies. Thus, there is no one single FDPR, but several FDPRs, which can be found in section 734.9 of the Export Administration Regulations.⁴⁷ FDPRs are most effective when targeting manufacturing technologies in which the United States is dominant, namely semiconductor manufacturing, and will not work in other sectors if U.S. equipment is not similarly present in all global manufacturing facilities.

While FDPRs have existed in export control policy for decades, the tool took on a new dimension when a novel FDPR was imposed on Huawei in 2020.⁴⁸ Earlier, the U.S. government had placed Huawei on the Entity List in May 2019, but this restriction did not prohibit U.S. and foreign companies from selling most foreign-made commercial items to Huawei from outside the United States.⁴⁹ The 2020 Huawei rule used an FDPR to dramatically expand the scope of controls on the shipment of goods to Huawei, including on an



extraterritorial basis, leveraging the critical role of U.S. firms in the global semiconductor supply chains, specifically related to semiconductor manufacturing equipment (i.e., tooling) and electronic design automation (EDA) software. Virtually no chip made anywhere in the world can be produced without using some U.S. tooling or EDA software. The Huawei FDPR leveraged this dominant U.S. market position to prohibit the sale to Huawei of any chip made anywhere in the world, if the chip was made using U.S. tooling or EDA software. This drastically shut off the supply of chips to Huawei.⁵⁰ At the time, this application of the FDPR could be viewed as a one-off move to address concerns of the Trump administration with Huawei.

However, once a tool has been developed, governments tend to use it. In 2022, the United States implemented a set of far-reaching FDPRs as part of efforts to sanction Russia following its 2022 invasion of Ukraine.⁵¹ The expanded use of FDPRs in this context was justified by the extraordinary nature of the crisis, with clear violations of international law requiring a strong response, ushering in the use of export controls as a sanctioning instrument. The United States reached for FDPRs yet again when imposing new controls on the export of advanced chips to China, as part of the aggressive controls released in October 2022 to stem China's advances in advanced chip production, AI, and supercomputing (the October 7 controls).⁵² The use of FDPRs in the October 7 controls indicates that FDPRs will now be used as a matter of course by administrations of both political parties when addressing a range of foreign policy and national security concerns.

Yet, it is not clear that FDPRs are having their intended effect. When faced with the controls, Huawei doubled down on investments in its own chip capacity, with some degree of success as the late 2023 release of the Huawei Mate 60 Pro phone using a Hi-Silicon designed, SMIC-fabricated 7 nanometer chip shows.⁵³ Russia continues to have access to a disconcerting level of Western chips.⁵⁴ FDPRs, which are inherently extraterritorial, are also controversial with key allies, who tend to chafe at the application of U.S. law in their jurisdictions. FDPRs are very difficult to investigate and enforce, as they involve commercial items that are made outside the United States, without any U.S.-origin content, manufactured by non-U.S. companies and sold to other non-U.S. companies. Further, FDPRs will eventually lose their bite if foreign firms begin to design out U.S. tooling to increase their autonomy to operate in a global chips marketplace without the constraint of U.S.-imposed controls. FDPRs are only relevant so long as the foreign firm continues to use the U.S. tooling, and eventually foreign fabs (including those outside of China) may replace U.S. tooling with that available from Dutch and Japanese competitors, thus rendering ineffective the future use of FDPRs.

As Congress considers strengthening the evaluation capacity of Commerce, it could prioritize the evaluation of these types of novel export controls. There is a keen need to understand how companies are responding to FDPR constraints. For Chinese firms, this should include an assessment of whether they are able to illicitly access U.S. chips in contravention of the FDPRs. It should also assess the extent to which FDPRs have spurred indigenous innovation in China. As importantly, the effect of extraterritorial measures on U.S. competitiveness, including the prospect of non-China foreign fabs designing out U.S. tooling, should be examined. Designing out of U.S. tooling is a completely legal and foreseeable consequence of extended extraterritorial measures. This means that the economic impact for U.S. tooling firms could be significant, as they lose access to a broader range of global markets, not just the China market.⁵⁵ Designing out may take years to occur, given the complexity of the technology involved, and thus U.S. assessments of potential impact should encompass both short- and long-term projections.

Export Control Data for External Researchers

External evaluation of the effectiveness of export controls is hampered by the lack of publicly available data, specifically data that enables one to analyze exports based on their export control classification. Researchers can approximate the flow of controlled goods using tariff codes, but tariff codes and export control classifications do not neatly align. This significantly complicates efforts to judge the effectiveness of current controls and to project the impact of new controls under consideration.



Exporters are required to report exports of certain items to the U.S. government, including all exports to China of items listed on the Commerce Control List.⁵⁶ This reported data on exports is analyzed by BIS and may inform its internal deliberations. However, very little information is released publicly, even in aggregated form. Congress could direct Commerce to study the feasibility of releasing substantially more export data publicly, including data that would enable external evaluation of trade flows by export control classification category. Data releases could be structured or aggregated in a manner that protects business confidential information.

V. Committee on Foreign Investment in the United States (CFIUS)⁵⁷

The United States has a well-established legal framework for screening certain foreign investments into U.S. businesses to address the national security risks that may arise from such transactions. These authorities are implemented by CFIUS, an interagency body chaired by the Secretary of the Treasury.⁵⁸ CFIUS has broad authority to respond to national security risks arising from foreign investments covered by its jurisdiction (*i.e.*, covered transactions).⁵⁹ “It can do this through the negotiation—or in some cases, imposition—of terms on a transaction to mitigate identified national security risks. Where mitigation cannot overcome the national security concerns, CFIUS may recommend that the president suspend or prohibit the covered transaction. The CFIUS program, implemented on a day-to-day basis by hundreds of civil servants working across the executive branch and subject to high levels of political accountability, is generally functioning well.”⁶⁰

In 2018, Congress provided substantial updates to the CFIUS process through the Foreign Risk Review Modernization Act of 2018 (FIRRMA), which passed in tandem with ECRA. FIRRMA updates included: an expansion of CFIUS jurisdiction to review new types of non-controlling investment transactions and greenfield real estate transactions; strengthening of mitigation and enforcement capabilities; streamlined filing requirements for certain transactions; and incentives for international partners to align their FDI screening mechanisms with CFIUS. Importantly, the FIRRMA reforms came with a corresponding increase in resources and staff for Treasury and other CFIUS agencies to implement their expanded responsibilities. Congressional attention to the question of resources has been critical to ensure that CFIUS can effectively implement FIRRMA and respond to a dynamic threat environment.

Post-FIRRMA, CFIUS generally has the legal authorities and institutional capacity it needs to address national security risks associated with foreign investments. However, Congress may wish to consider a series of targeted updates to address evolving threats related to technology competition with China. Specifically, Congress may wish to expand the CFIUS definition of critical technologies to strengthen CFIUS jurisdiction over transactions involving emerging technologies. It could also consider a stronger oversight role in addressing high case volumes and potential mission creep of CFIUS, which may be over-burdening the CFIUS process and diverting resources from technology-related transactions.

Expansion of Critical Technology Definition

CFIUS has traditionally defined “critical technology” through reference to the export control authorities, rather than developing its own lists of sensitive technologies. For a technology to be considered a critical technology for CFIUS purposes, the technology must have been identified and listed by the export controls agencies on one of the U.S. export control lists (*e.g.*, the U.S. Munitions List or the Commerce Control List).⁶¹ Prior to FIRRMA, this definitional issue had little practical impact. CFIUS had—and continues to have—full jurisdiction to review any transaction that conveys “control,” as defined in FIRRMA, over the U.S. business to the foreign investor, regardless of whether the U.S. business engages in critical technology or not.⁶² “Under FIRRMA, however, the definition of critical technology took on heightened importance in two ways. First, new CFIUS jurisdiction over covered investments (*i.e.*, investments that conveyed important benefits, short of full control, to the foreign investor) was limited to only certain types of U.S. businesses, including those



that engaged in critical technology as defined through reference to export control authorities. Second, the new FIRRMA authorities to mandate notifications of certain transactions to CFIUS also hinged on the definition of critical technology. These changes gave new importance to the linkage between export control authorities and CFIUS.⁶³

Consistency between CFIUS and export controls is generally a best practice, as it enhances policy coherence across the various authorities and facilitates private sector compliance. However, in certain cases, risks that arise from an investment transaction may differ meaningfully from risks arising from an export. Export risks relate to an adversary gaining new access to a technology that has national security relevance. In contrast, investment risks may include a much broader range of potential risk scenarios, including those related to the foreign investor's access to privileged information about a U.S. business or the ability to influence decisions of that business.

Artificial intelligence is a useful case study for assessing the different types of risks arising from exports and investment transactions. Frontier AI systems (i.e., often defined as general-purpose systems at the frontier of AI research and development) are showing increasing capabilities to mimic human cognitive abilities and learn new skills through ingesting and analyzing massive amounts of data. Though these systems retain many rough edges, there are already indications of potential national security harms that could arise from misuse, including the enabling of cyberattacks, spreading disinformation, conducting weapons testing, or developing novel toxins.⁶⁴ Many experts are concerned that these same capabilities could lead to catastrophic outcomes, either via accident or deliberate misuse.⁶⁵ How frontier AI systems are developed to guard against these risks is inherently a matter of governance, and governance is deeply reliant on the interests, values, and ethics of the individuals in charge of AI companies. CFIUS should have broad jurisdiction to review how foreign investors may influence these governance dynamics, regardless of whether the U.S. business “produces, designs, tests, manufactures, fabricates, or develops” technology that is currently subject to U.S. export controls (i.e., whether the U.S. business meets the FIRRMA definition of engaging in critical technologies).⁶⁶ Currently, AI export controls are very limited and largely confined to AI chips. AI companies (either frontier AI labs or other start-ups that leverage AI systems built by these labs) do not always make their own chips and thus would likely not be caught by current CFIUS jurisdiction. Enabling CFIUS to identify and remedy these sorts of scenarios can address jurisdictional gaps and allow for more robust oversight into the range of risks that foreign investments into U.S. emerging technology ecosystems can present.

Specifically, Congress could expand the definition of “critical technologies” in FIRRMA to include a new category of “technologies controlled for investment purposes.” This new category would be additional to the existing definitions. Congress could require CFIUS to issue regulations within one year to identify those technologies that would be defined as “technologies controlled for investment purposes” and direct them to consider all technologies listed as critical and emerging technologies by the White House Office of Science and Technology Policy.⁶⁷ Finally, Congress could provide guidance to CFIUS that for transactions involving “technologies controlled for investment purposes,” CFIUS should consider all national security risks that may arise from the foreign investor's involvement in the transaction, including how the foreign investor may shape the use and deployment of the technology. The new authorities should be narrowly targeted at investments from competitor nations, to avoid chilling beneficial investment from U.S. partners and allies.

High Case Volumes and Potential for Mission Creep

CFIUS is reviewing historically high numbers of transactions. In 2022, the most recent year for which Treasury has reported data, CFIUS reviewed 154 short-form declarations and 286 notices.⁶⁸ This is roughly double the number of transactions that CFIUS reviewed pre-FIRRMA. CFIUS is also negotiating or imposing mitigation terms on transactions at historically high levels, with 41 mitigation agreements for transactions filed in 2022—the highest amount in the post-FIRRMA period.⁶⁹ These increasing case volumes require continued congressional attention to ensure that CFIUS has the budget and staffing in all CFIUS



agencies to carry out CFIUS responsibilities. This is essential both to address urgent national security risks, as well as to ensure that beneficial investments can clear the CFIUS process in a predictable and expeditious manner, consistent with the U.S. open investment policy.

The high case volumes are driven in part by the increased expansion of jurisdiction under FIRRMA, but they are also a result of CFIUS stepping in to fill gaps in other authorities. The most pronounced area in which CFIUS is filling a policy void is related to data privacy and data security. In the absence of national legislation to provide robust data privacy protections for individuals and to regulate the transfers of sensitive bulk data overseas, CFIUS is often left to use its mitigation authorities to address data risks that appear in the context of a foreign investment simply because it is the only authority available to do so. CFIUS is intended to be a tool of last resort, and it is not designed to address all risks that may be present in the U.S. economy. Instead, when it comes to data privacy and security, CFIUS “has become a tool of convenience to impose a patchwork of protections for sensitive data held by companies that just so happen to be receiving a foreign investment.”⁷⁷⁰

As noted in prior testimony, “Congress can help by passing comprehensive data privacy and data security legislation. Data privacy objectives should include giving individuals greater control over what data is collected about them online and how that information is sold or used. Data security objectives should address the national security concerns that can arise from the bulk transfer of sensitive data to a foreign adversary. Data privacy and data security have overlapping objectives and stronger data privacy will inherently reduce data security risks through minimization of the personal data on the open market. Data privacy and data security legislation is important in its own right but will also help return CFIUS to its intended purposes of addressing foreign investment risks rather than dealing with data risks writ large.”⁷⁷¹

CFIUS’s assessment of third-party risks represent another area in which CFIUS may be over-extended. Third-party risks arise when a foreign investor’s relationships with competitor nations, rather than the foreign investor itself, that raise concerns. For example, CFIUS may be concerned if a European company with extensive business operations in China is acquiring a sensitive U.S. business, as the technology of the U.S. business could indirectly leak to China post-investment. The high level of mitigation agreements in 2022, paired with an overall decline in Chinese investment in the United States, may be an indicator that mitigation agreements are increasingly being used for third-party risk.⁷⁷² While CFIUS has clear authority to address such concerns, it would be far more effective if U.S. partners and allies strengthened their own economic security toolkits to address these concerns directly in their own jurisdictions. While the Departments of Treasury and State have made admirable strides in encouraging FDI screening in partner and allied countries, many of these mechanisms remain less mature than the CFIUS and coordination with the United States on assessing investment risks varies significantly by country.

Congress could remedy these issues by providing robust resources to the investment security international outreach functions in Treasury and State. Additionally, Congress has an important oversight role to ensure that aggressive CFIUS mitigation of investments from U.S. partners and allies is not chilling the U.S. investment climate or straining U.S. alliances. Congress could institute “a new requirement for CFIUS to assess and report to Congress on the impact of the CFIUS process on foreign investment flows from allies and partners. This should include assessment of whether these flows have been negatively impacted by FIRRMA’s expansion of CFIUS jurisdiction and whether FIRRMA’s tools to address this, including the exempted foreign state program and the declaration process, are being effectively utilized. The reporting requirement should also address the impact of mitigation agreements on the investments of allies and partners, with the aim of ensuring that these mitigation agreements are genuinely focused on risks arising from the transaction and attributable to the foreign investor, rather than broader systemic risks.”⁷⁷³ Congress may also want to consider strengthening the role of the Office of Legal Counsel (OLC) within the CFIUS process, to guard against potential mission creep and ensure that all CFIUS decisions could withstand external or judicial review.⁷⁷⁴



VI. Outbound Investment Controls⁷⁵

U.S. policymakers are currently debating whether and how to regulate U.S. investments in China (i.e., outbound investment). The administration has released an executive order, with an accompanying advanced notice of proposed rulemaking (ANPRM), outlining a targeted proposal to mandate notifications of—and in some cases, prohibit—certain U.S. investments into China’s AI, semiconductor, and quantum technology ecosystems.⁷⁶ Congress has considered a range of proposals, with current efforts in the Senate coalescing around a mandatory notification program.⁷⁷ Debate remains ongoing in the House of Representatives, with the House Financial Services Committee advancing legislation that leans more heavily on traditional sanctions tools to address concerns with outbound investment.⁷⁸ The House Select Committee on the Strategic Competition between the United States and the Chinese Communist Party, in its recent report on the U.S.-China economic relationship, has recommended new authorities to implement a sectoral approach to regulating outbound investment.⁷⁹

The following analysis and recommendations draw from joint work conducted by the author and Sarah Bauerle Danzman, including the report *Sand in the Silicon: Designing an Outbound Investment Mechanism* published jointly by the Atlantic Council and CNAS.⁸⁰ Highlights of *Sand in the Silicon* are provided here, and additional detail and analysis can be found in the report. Dr. Danzman testified before the Committee on September 29, 2022 in the hearing titled “Examining Outbound Investment.”

The National Security Case for Regulating Outbound Investment

Certain U.S. investments in China present national security risks that are not addressed by existing U.S. authorities. U.S. firms and investors may, in some cases, be supporting the development of critical technologies in China that have important national security applications. These include investments related to chips, AI, or other technologies that can accelerate advances in Chinese military capabilities.⁸¹ Just as U.S. law and policy have long recognized that the export of certain technologies can be counter to U.S. security interests, so too can certain overseas investments if such investments are contributing to increasing military capabilities of competitor nations. While officials have raised a wide range of concerns related to U.S. investment in China, including related to human rights, offshoring of U.S. jobs, and financial stability, outbound investment controls would not be appropriate in each of these areas.⁸² The goal of an outbound investment program is not to impose broad capital controls, but to instead address the specific transactions through which critical industrial knowhow may transfer to China and to plug a specific gap that export controls cannot fill in the technology competition with China.

Outbound investment controls can be best thought of as a complement to U.S. export controls, filling a gap related to non-technical expertise that export controls are ill suited to capture. Export controls address part of the national security risk associated with outbound investments, namely the risk that investments may involve the transfer of sensitive U.S. technologies. However, export controls do not cover the full range of risks associated with outbound investment transactions, particularly those that arise from the transfer of management expertise or other non-technical industrial knowhow. For example, one can consider the broad range of skills and expertise needed to establish and operate a semiconductor fabrication facility that can produce high-quality chips at scale and on commercially competitive terms. Technical knowledge and technology innovation will be critical to this business, and export controls can address this aspect of potential risk associated with U.S. investments into China-based facilities. But, the operators of these facilities will also need to manage complex supply chains, maintain a skilled workforce, and develop commercial strategies for succeeding in a cutthroat global marketplace. Few companies today can master these complex operational and management requirements. This type of management expertise is one example of the non-technology related benefits that can flow along with an outbound investment that are not, and never would be, suitable to capture under export control authorities.



Designing New Outbound Investment Controls

Addressing national security risks associated with U.S. investments in China will require a carefully calibrated approach. Overarching principles guiding the development of future outbound investment tools should include that such tools should be:

- targeted at transactions of highest national security risk;
- clearly defined and understandable to private-sector entities, who will be responsible for the first line of compliance;
- non-duplicative of and consistent with existing tools, including export controls;
- scoped proportionately to the administrative capacity available to effectively administer a new mechanism; and
- designed to enable meaningful conversations with allies about adopting similar regimes, including the need to limit extraterritorial application of U.S. authorities.⁸³

Consistent with these broad principles, the United States should focus on U.S. investments that: 1) convey management expertise or other industrial knowhow along with the investment; 2) are made into critical technology sectors in China; and 3) may advance the indigenous development of China's technology capabilities in areas relevant to national security.

Given the complexity of the investment environment in China, the United States will need a multi-pronged approach to adequately address the national security risks associated with certain U.S. investments in China. This should include:

- **Mandatory notification requirements:** The U.S. government does not have full visibility into the entire scope of investment transactions being made by U.S. investors in China. Existing data sources are often too aggregated or incomplete, providing little information on the critical technologies involved in investment transactions. Recent Chinese efforts to crack down on Western due diligence firms further complicate attempts to understand the investment environment. Mandatory requirements to notify a defined scope of transactions to the U.S. government, subject to strict confidentiality requirements, is an important tool that can inform the design and administration of an effective outbound investment regime. Both the U.S. Senate and the administration have put forth proposals for notification requirements, though neither is yet in effect.⁸⁴
- **Prohibitions of investments into high-risk technologies or sectors:** The U.S. government should prohibit U.S. investments in sectors in China that have clear military relevance. The government could establish a prohibition on U.S. investments in any Chinese firm that produces, designs, tests, manufactures, fabricates, or develops any technology that meets the technical specification of a technology that is subject to a U.S. arms embargo with respect to China, which would capture items on the U.S. Munitions List as well as space and military items listed on the Commerce Control List.⁸⁵ Additionally, prohibitions could be considered for investments into Chinese firms making other technologies subject to high levels of export controls, such as advanced semiconductors that meet the technical thresholds set in the October 7 controls. These sorts of prohibitions have an inherent logic, as U.S. persons should not be able to financially support Chinese indigenous development of the exact technologies that are prohibited from export to China.
- **Entity-based restrictions:** The U.S. government should establish authorities to prohibit U.S. investments into particular Chinese entities, as a complement to a sector-based notification and prohibition requirements. This allows for stronger action with respect to specific entities that the U.S. government may identify as acting against U.S. national security or foreign policy interests. The government has certain entity-based investment restrictions under the Chinese Military-Industrial



Complex (non-SDN CMIC) program. However, this authority is limited to the purchase or sale of publicly listed companies. Expansion of this program to include all types of investment transactions, as well as authorizing the designation of companies that are supporting Chinese indigenous development of national security technologies, can strengthen overall efforts to address investment-related national security risks. While certain policymakers have advocated for the use of full blocking sanctions to address outbound concerns, the use of this more severe form of sanction is highly escalatory and can exacerbate dedollarization risks.⁸⁶ Premature use of full blocking sanctions will erode the power of the U.S. sanctions threat over China, which should be preserved for moments of acute crisis or conflict.⁸⁷

- **End use restrictions:** The U.S. government should establish investment restrictions based on the intended end use of the technology of the invested Chinese company. For example, U.S. investments should not be permitted into Chinese companies developing technologies with military, intelligence, or mass surveillance end uses. End use restrictions can complement sectoral and entity-based restrictions, mirroring a similar construct in export controls, which include list-based, end use, and end user controls. Crafting end use controls, however, must reflect the inherently dual-use nature of many technologies that are at the heart of the U.S.-China competition. For example, the administration's executive order includes an end use rule related to the development of AI systems for exclusively military end use, which is an unhelpfully narrow scope and would miss key AI labs in China, as frontier models today are inherently dual use.⁸⁸

Congress has an essential role in establishing any new outbound investment authorities. While substantively the administration's executive order generally aligns with the recommendations of this testimony, implementing these authorities under executive action is not optimal over the longer term. Congress should act to codify and shape new outbound investment authorities, as well as to appropriate necessary resources and to conduct rigorous oversight to ensure that the authorities are being implemented effectively to advance U.S. national security interests.

VII. Conclusion

The United States faces a new era of strategic competition with China, one that presents challenges fundamentally different than prior eras due to China's essential role in the global economy. U.S. policy must account for objectives in tension with one another, including the need to de-risk economic ties that present pronounced national security risks while maintaining those ties that are in the U.S. strategic interest and ensuring the stability of the global economy. Navigating these difficult waters requires a clear strategic vision, bureaucratic orientation toward the China challenge, and a clear-eyed assessment of whether current U.S. policies are working. This analysis and recommendations in this testimony are intended to further these goals.

VIII. Additional Analysis

The following reports and analysis are cited in this testimony and are highlighted here for the convenience of the Committee in its future work.

Sarah Bauerle Danzman and Emily Kilcrease, "The Illusion of Controls: Unilateral Attempts to Contain China's Technology Ambitions Will Fail," *Foreign Affairs*, December 30, 2022, <https://www.foreignaffairs.com/united-states/illusion-controls>.

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



Emily Kilcrease, *No Winners in This Game: Assessing the U.S. Playbook for Sanctioning China* (Washington, D.C.; Center for a New American Security, December 1, 2023), https://cs3.us-east-1.amazonaws.com/files.cnas.org/documents/EES-No-Winners_Final-1.pdf.

Challenging China's Trade Practices: Promoting Interests of U.S. Workers, Farmers, Producers, and Innovators Hearing Before the U.S.-China Economic and Security Review Commission (2022) (statement of Emily Kilcrease, Senior Fellow and Director of the Energy, Economics, and Security Program, CNAS), <https://www.cnas.org/publications/congressional-testimony/challenging-chinas-trade-practices>.

The Role of Investment Security in Addressing China's Pursuit of Defense Technologies: Hearing Before the U.S.-China Economic and Security Review Commission, 118th Cong. (2023) (statement of Emily Kilcrease, Senior Fellow and Director, Energy, Economics, and Security Program, CNAS), https://www.uscc.gov/sites/default/files/2023-04/Emily_Kilcrease_Testimony.pdf.

Emily Kilcrease, Jasper Helder, and Kevin Wolf, *Public Comments of Kevin Wolf, Emily Kilcrease, and Jasper Helder Regarding Areas and Priorities for US and EU Export Control Cooperation under the US-EU Trade and Technology Council* (January 14, 2022), www.cnas.org/publications/commentary/public-comments-kilcrease-us-and-eu-export-control-cooperation-under-the-us-eu-trade-and-technology-council.

Emily Kilcrease and Michael Frazer, *Sanctions by the Numbers: SDN, CMIC, and Entity List Designations on China* (Washington, D.C.; Center for a New American Security, March 2, 2023), <https://www.cnas.org/publications/reports/sanctions-by-the-numbers-sdn-cmic-and-entity-list-designations-on-china>.

Emily Kilcrease, Tim Fist, Sarah Bauerle Danzman, Ngor Luong, and Emily Weinstein, *Comments on Provisions Pertaining to U.S. Investments in Certain National Security Technologies and Products in Countries of Concern* (September 29, 2023), <https://www.cnas.org/publications/commentary/comments-on-provisions-pertaining-to-u-s-investments-in-certain-national-security-technologies-and-products-in-countries-of-concern>.

Emily Kilcrease, *Noteworthy: The New Russia Export Controls* (Washington, D.C.; Center for a New American Security, March 7, 2022), <https://www.cnas.org/press/press-note/noteworthy-the-new-russia-export-controls>.

Emily Kilcrease, "How to Win Friends and Choke China's Chip Supply," *War on the Rocks*, Metamorphic Media, January 6, 2023, <https://warontherocks.com/2023/01/how-to-win-friends-and-choke-chinas-chip-supply/>.

Emily S. Weinstein and Ngor Luong, *U.S. Outbound Investment into Chinese AI Companies* (Center for Security and Emerging Technologies, February 2023), <https://cset.georgetown.edu/publication/u-s-outbound-investment-into-chinese-ai-companies/>.

Stacie Pettyjohn and Becca Wasser, *No I in Team: Integrated Deterrence with Allies and Partners* (Washington, D.C.; Center for a New American Security, December 14, 2022), <https://www.cnas.org/publications/reports/no-i-in-team>.

Onni Aame, Tim Fist, and Caleb Withers, *Secure, Governable Chips: Using On-Chip Mechanisms to Manage National Security Risks from AI & Advanced Computing* (Washington, D.C.; Center for a New American Security, January 8, 2024), <https://www.cnas.org/publications/reports/secure-governable-chips>.

Tim Fist and Enich Grunewald, *Preventing AI Chip Smuggling to China: A Working Paper* (Washington, D.C.; Center for a New American Security, October 24, 2023), <https://www.cnas.org/publications/reports/preventing-ai-chip-smuggling-to-china>.



- ¹ Antony J. Blinken, "The Administration's Approach to the People's Republic of China" (speech, The George Washington University, Washington, D.C., May 26, 2022), <https://www.state.gov/the-administrations-approach-to-the-peoples-republic-of-china/>.
- ² Juan Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare* (New York: PublicAffairs, 2019).
- ³ U.S. Department of Defense, *National Defense Industrial Strategy* (U.S. Department of Defense, January 11, 2024), <https://www.businessdefense.gov/docs/ndis/2023-NDIS.pdf>; Deputy Secretary of Commerce Don Graves, "Remarks by Deputy Secretary of Commerce Don Graves at the National Foreign Trade Council's Alliance for National Security and Competitiveness" (public event, National Foreign Trade Council, Washington, D.C., January 9, 2024), <https://www.commerce.gov/news/speeches/2024/01/remarks-deputy-secretary-commerce-don-graves-national-foreign-trade-councils-alliance-for-national-security-and-competitiveness>.
- ⁴ U.S. Department of the Treasury, *The Treasury 2021 Sanctions Review* (U.S. Department of the Treasury, October 2021), <https://home.treasury.gov/system/files/136/Treasury-2021-sanctions-review.pdf>.
- ⁵ Zach Cooper, "Does America Have an Endgame on China?" *ChinaFile*, December 15, 2023, <https://www.asi.org/cp-eds/does-america-have-an-endgame-on-china/>.
- ⁶ Emily Kilcrease, *No Winners in This Game: Assessing the U.S. Playbook for Sanctioning China* (Washington, D.C.: Center for a New American Security, December 1, 2023), https://csur.org/americansecurity.com/files/cnas.org/documents/EBS-No-Winners_Final1.pdf.
- ⁷ U.S. National Security Strategy (Washington, D.C.: White House, October 2022), <https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administration-National-Security-Strategy-10-2022.pdf>.
- ⁸ Secretary of the Treasury Janet Yellen, "Remarks by Secretary of the Treasury Janet L. Yellen on the U.S.-China Economic Relationship" (public event, Johns Hopkins School of Advanced International Studies, Washington, D.C., April 20, 2023), <https://home.treasury.gov/news/press-releases/pl1425>.
- ⁹ Secretary of Commerce Gina Raimondo, "Remarks by U.S. Secretary of Commerce Gina Raimondo on U.S. Competitiveness and the China Challenge" (public event, Massachusetts Institute of Technology, Cambridge, MA, November 30, 2022), <https://www.commerce.gov/news/speeches/2022/11/remarks-us-secretary-commerce-gina-raimondo-us-competitiveness-and-china>.
- ¹⁰ Jake Sullivan, "Remarks by National Security Advisor Jake Sullivan on Renewing American Economic Leadership" (public event, Brookings Institution, Washington, D.C., April 27, 2023), <https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/04/27/remarks-by-national-security-advisor-jake-sullivan-on-renewing-american-economic-leadership-at-the-brookings-institution/>; and Blinken, "The Administration's Approach to the People's Republic of China."
- ¹¹ Representative Mike Gallagher, "Let's Stop Paying Beijing to Steal Our Gene Code," press release, November 13, 2023, <https://gallagher.house.gov/media/in-the-news/lets-stop-paying-beijing-steal-our-gene-code>.
- ¹² For more on "integrated deterrence," see 2022 *National Defense Strategy of the United States of America* (U.S. Department of Defense, October 27, 2022), <https://media.defense.gov/2022/Oct/27/2023103845/1/1/2022-NATIONAL-DEFENSE-STRATEGY-NFR/MDR/EDF>.
- ¹³ Stacie Pettyjohn and Becca Wasser, *No I in Team: Integrated Deterrence with Allies and Partners* (Washington, D.C.: Center for a New American Security, December 14, 2022), <https://www.cnas.org/publications/reports/no-i-in-team>.
- ¹⁴ Sarah Bautele Danzman and Emily Kilcrease, "The Illusion of Controls: Unilateral Attempts to Contain China's Technology Ambitions Will Fail," *Foreign Affairs*, December 30, 2022, <https://www.foreignaffairs.com/united-states/illusion-controls>.
- ¹⁵ Hugo Meijer, *Trading with the Enemy: The Making of US Export Control Policy toward the People's Republic of China* (New York: Oxford University Press, 2016); Tim Huang and Emily Weinstein, *Decoupling in Strategic Technologies: From Satellites to Artificial Intelligence* (Center for Security and Emerging Technology, July 2022), <https://cset.georgetown.edu/publication/decoupling-in-strategic-technologies/>.
- ¹⁶ Emily Weinstein and Kevin Wolf, "COCOM's Daughter?", World ECR, May 13, 2022, <https://cset.georgetown.edu/article/cocoms-daughter/>.
- ¹⁷ *Challenging China's Trade Practices: Promoting Interests of U.S. Workers, Farmers, Producers, and Innovators: Hearing Before the U.S.-China Economic and Security Review Commission* (2022) (statement of Emily Kilcrease, Senior Fellow and Director of the Energy, Economics, and Security Program, CNAS), <https://www.cnas.org/publications/congressional-testimony/challenging-chinas-trade-practices>.
- ¹⁸ Kilcrease, *No Winners in This Game: Assessing the U.S. Playbook for Sanctioning China*; Emily Benson and Catharine Mouradian, *Establishing a New Multilateral Export Control Regime* (Center for Strategic and International Studies, November 2, 2023), <https://www.csis.org/analysis/establishing-new-multilateral-export-control-regime>.
- ¹⁹ Emily Kilcrease, Jasper Helder, and Kevin Wolf, *Public Comments of Kevin Wolf, Emily Kilcrease, and Jasper Helder Regarding Areas and Priorities for US and EU Export Control Cooperation under the US-EU Trade and Technology Council* (January 14, 2022), <https://www.cnas.org/publications/commentary/public-comments-kilcrease-us-and-eu-export-control-cooperation-under-the-us-eu-trade-and-technology-council>.
- ²⁰ The White House, "G7 Leaders' Statement on Economic Resilience and Economic Security," press release, May 20, 2023, <https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/g7-leaders-statement-on-economic-resilience-and-economic-security/#:~:text=G7%20Leaders%20Statement%20on%20Economic%20Resilience%20and%20Economic%20Security,Home&text=Fostering%20>.
- ²¹ Kilcrease, *Challenging China's Trade Practices: Promoting Interests of U.S. Workers, Farmers, Producers, and Innovators: Hearing Before the U.S.-China Economic and Security Review Commission*.
- ²² Kilcrease, Helder, and Wolf, *Public Comments of Kevin Wolf, Emily Kilcrease, and Jasper Helder Regarding Areas and Priorities for US and EU Export Control Cooperation under the US-EU Trade and Technology Council*.
- ²³ Emily Kilcrease and Michael Frazer, *Sanctions by the Numbers: SDN, CMIQ, and Entity List Designations on China* (Washington, D.C.: Center for a New American Security, March 2, 2023), <https://www.cnas.org/publications/reports/sanctions-by-the-numbers-sdn-cmiq-and-entity-list-designations-on-china>.
- ²⁴ In full disclosure, the author is employed by a think tank and the author's spouse is employed by a federally funded research and development center.
- ²⁵ For ECR's statement of policy, see Export Control Reform Act of 2018, 50 U.S.C. § 4811, (2018), <https://uscode.house.gov/view.xhtml?path=/prelim@title50/chapter58&edition=prelim>.
- ²⁶ *Advancing National Security and Foreign Policy Through Sanctions, Export Controls, and Other Economic Tools: Hearing Before the Senate Committee on Banking, Housing, and Urban Affairs*, 118th Cong. 4-5 (2023) (Statement of Kevin Wolf, Non-Resident Senior Fellow at the Center for Security and Emerging Technology), <https://www.banking.senate.gov/imo/media/doc/Wolf%20Testimony%2002-28-23.pdf>.



- 21

- ⁵³ Danzman and Kilcrease, "Illusion of Controls: Unilateral Attempts to Contain China's Technology Ambitions Will Fail."
- ⁵⁴ See 15 CFR § 758.1, "The Electronic Export Information (EEI) filing to the Automated Export System (AES)," <https://www.law.cornell.edu/cfr/text/15/758.1>.
- ⁵⁵ Analysis and recommendations in this section draw from prior testimony provided by the U.S.-China Economic and Security Review Commission, see *The Role of Investment Security in Addressing China's Pursuit of Defense Technologies: Hearing Before the U.S.-China Economic and Security Review Commission*, 118th Cong. (2023) (statement of Emily Kilcrease, Senior Fellow and Director, Energy, Economics, and Security Program, CNAS), https://www.uscc.gov/sites/default/files/2023-04/Emily_Kilcrease_Testimony.pdf.
- ⁵⁶ For an overview of the CFIUS interagency process, see the CFIUS website at <https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius>.
- ⁵⁷ See 31 CFR § 800.213 (*covered transaction*).
- ⁵⁸ Kilcrease, *The Role of Investment Security in Addressing China's Pursuit of Defense Technologies: Hearing Before the U.S.-China Economic and Security Review Commission*.
- ⁵⁹ See 50 USC § 4565(a)(6) and 31 CFR § 800.215.
- ⁶⁰ See 31 CFR § 800.210 (*covered controls transaction*).
- ⁶¹ Kilcrease, *The Role of Investment Security in Addressing China's Pursuit of Defense Technologies: Hearing Before the U.S.-China Economic and Security Review Commission*.
- ⁶² Fabio Urbina, Filippa Lentzos, Cédric Invernizzi, and Sean Ekins, "Dual use of artificial-intelligence-powered drug discovery," *Nature Machine Intelligence*, 4, March 2022.
- ⁶³ Cade Metz and Gregory Schmidt, "Elon Musk and Others Call for Pause on A.I., Citing 'Profound Risks to Society,'" *The New York Times*, March 29, 2023, <https://www.nytimes.com/2023/03/29/technology/ai-artificial-intelligence-musk-risks.html>.
- ⁶⁴ See 31 CFR § 800.248 (*TID U.S. business*).
- ⁶⁵ National Science and Technology Council, *Critical and Emerging Technologies List Update: A Report by the Fast Track Action Subcommittee on Critical and Emerging Technologies*.
- ⁶⁶ U.S. Department of the Treasury, "Committee on Foreign Investment in the United States: Annual Report to Congress, Report Period CY 2022" (U.S. Department of the Treasury, 2023), https://home.treasury.gov/system/files/206/CFIUS%20-%20Annual%20Report%20to%20Congress%20CY%202022_6.pdf.
- ⁶⁷ U.S. Department of the Treasury, "Committee on Foreign Investment in the United States: Annual Report to Congress, Report Period CY 2022" (U.S. Department of the Treasury, 2023), https://home.treasury.gov/system/files/206/CFIUS%20-%20Annual%20Report%20to%20Congress%20CY%202022_6.pdf.
- ⁶⁸ Kilcrease, *The Role of Investment Security in Addressing China's Pursuit of Defense Technologies: Hearing Before the U.S.-China Economic and Security Review Commission*.
- ⁶⁹ Kilcrease, *The Role of Investment Security in Addressing China's Pursuit of Defense Technologies: Hearing Before the U.S.-China Economic and Security Review Commission*.
- ⁷⁰ U.S. Department of the Treasury, "Committee on Foreign Investment in the United States: Annual Report to Congress, Report Period CY 2022"; Thile Hanemann, Armand Meyer, and Danielle Goh, "Vanishing Act: The Shrinking Footprint of Chinese Companies in the US," Rhodium Group, September 7, 2023, <https://thg.com/research/vanishing-act-the-shrinking-footprint-of-chinese-companies-in-the-us/>.
- ⁷¹ Kilcrease, *The Role of Investment Security in Addressing China's Pursuit of Defense Technologies: Hearing Before the U.S.-China Economic and Security Review Commission*.
- ⁷² Kilcrease, *The Role of Investment Security in Addressing China's Pursuit of Defense Technologies: Hearing Before the U.S.-China Economic and Security Review Commission*.
- ⁷³ Analysis and recommendations in this section draw heavily on joint work conducted with Sarah Bauele Danzman, as published in Sarah Bauele Danzman and Emily Kilcrease, *Sand in the Silt: Designing an Outbound Investment Controls Mechanism* (Washington, D.C.: The Atlantic Council, September 14, 2022), <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/sand-in-the-silt-on-designing-an-outbound-investment-controls-mechanism>.
- ⁷⁴ White House, *Executive Order on Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern*, Washington, D.C., August 9, 2023, <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/08/09/executive-order-on-addressing-united-states-investments-in-certain-national-security-technologies-and-products-in-countries-of-concern/>.
- ⁷⁵ Karen Freifeld and Andrea Shalal, "US senators push China investments tracker in defense bill as White House finalizes order," Reuters, July 14, 2023, <https://www.reuters.com/world/us/us-senators-push-china-investments-tracker-defense-bill-white-house-finalizes-2023-07-14/>.
- ⁷⁶ U.S. House of Representatives Financial Services Committee, "McHenry, Subcommittee Chairs Urge House and Senate Armed Services Committee Leadership to Reject Misguided Outbound Investment Regime, Prioritize Time-Tested Sanctions and Export Controls," press release, November 29, 2023, <https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=409061>.
- ⁷⁷ The Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, *Reset, Prevent, Build: A Strategy to Win America's Economic Competition with the Chinese Communist Party* (Washington, D.C.: U.S. House of Representatives, Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, December 12, 2023), <https://selectcommitteesthecp.house.gov/sites/ero-sites/selectcommitteesthecp.house.gov/files/ero-media-document/reset-prevent-build-go-report.pdf>.
- ⁷⁸ Danzman and Kilcrease, *Sand in the Silt: Designing an Outbound Investment Controls Mechanism*.
- ⁷⁹ Emily S. Weinstein and Ngor Luong, *U.S. Outbound Investment into Chinese AI Companies* (Center for Security and Emerging Technologies, February 2023), <https://cset.georgetown.edu/publication/us-a-outbound-investment-into-chinese-ai-companies/>; and Alex Alpers and Eduardo Baptista, "China chip firm powered by US tech and money avoids Biden's crackdown," Reuters, December 13, 2023, <https://www.reuters.com/technology/china-chip-firm-powered-by-us-tech-money-avoids-bidens-crackdown-2023-12-13/>.
- ⁸⁰ Danzman and Kilcrease, *Sand in the Silt: Designing an Outbound Investment Controls Mechanism*.
- ⁸¹ Danzman and Kilcrease, *Sand in the Silt: Designing an Outbound Investment Controls Mechanism*.
- ⁸² White House, *Executive Order on Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern*, and Karen Freifeld and Andrea Shalal, "US senators push China investments tracker in defense bill as White House finalizes order."
- ⁸³ Danzman and Kilcrease, *Sand in the Silt: Designing an Outbound Investment Controls Mechanism*.
- ⁸⁴ U.S. House of Representatives Financial Services Committee, "McHenry, Subcommittee Chairs Urge House and Senate Armed Services Committee Leadership to Reject Misguided Outbound Investment Regime, Prioritize Time-Tested Sanctions and Export Controls."



⁸⁷ Kilcrease, *No Winners in This Game: Assessing the U.S. Playbook for Sanctioning China*; Emily Kilcrease and John Hughes, “It’s not time to hit China with financial sanctions – yet,” *The Hill*, January 16, 2024, <https://thehill.com/opinion/international/4411407-its-not-time-to-hit-china-with-financial-sanctions-yet/>.

⁸⁸ Emily Kilcrease, Tim Fist, Sarah Baetle Danzman, Ngoc Luong, and Emily Weinstein, *Comments on Provisions Pertaining to U.S. Investments in Certain National Security Technologies and Products in Countries of Concern*.



PREPARED STATEMENT OF JAMIL N. JAFFER
FOUNDER AND EXECUTIVE DIRECTOR, NATIONAL SECURITY INSTITUTE AND NSI CYBER
AND TECH CENTER, ANTONIN SCALIA LAW SCHOOL AT GEORGE MASON UNIVERSITY
JANUARY 18, 2024

Statement for the Record
of
Jamil N. Jaffer¹
on
National Security Challenges: Outpacing China in Emerging Technology
before the
United States Senate Committee on Banking, Housing, and Urban Affairs
January 18, 2024

I. Introduction

Chairman Brown, Ranking Member Scott, and Members of the Committee: thank you for inviting me here today to discuss the national security challenges facing our nation when it comes the pursuit of emerging technologies and specifically, the very real threat posed by People's Republic of China (PRC) under the leadership of the Chinese Communist Party (CCP) in this domain.²

I want to thank Chairman Brown and Ranking Member Scott for holding this hearing in the context of the Banking Committee's work and oversight responsibilities and, in particular, I want to thank both of you for your leadership in highlighting the significant relationship between national security and emerging technologies, particularly as we think about investment and innovation in the context of the threat posed by the PRC. As you both know, China is the key economic and national security challenge facing our nation going forward and our nation's ability to rapidly innovate is—and will remain—central to our ability to effectively address this challenge. I also want to thank both of you for your leadership in moving forward bipartisan legislative initiatives on challenges related to China, including addressing the very real national security threat posed by Fentanyl coming from the PRC through our southern border. I hope this hearing will offer us the opportunity to have a candid and frank discussion on these important matters.

¹ Jamil N. Jaffer currently serves as Founder & Executive Director of the National Security Institute and the NSI Cyber and Tech Center and as an Assistant Professor of Law and Director of the National Security Law & Policy and Cyber, Intelligence and National Security Programs at the Antonin Scalia Law School at George Mason University. Mr. Jaffer is also a Venture Partner at Paladin Capital Group, a leading global multi-stage investor that identifies, supports and invests in innovative companies that develop promising, early-stage technologies to address the critical cyber and advanced technological needs of both commercial and government customers. Among other things, Mr. Jaffer previously served as Chief Counsel & Senior Advisor to the Senate Foreign Relations Committee, Senior Counsel to the House Intelligence Committee, Associate Counsel to President George W. Bush in the White House, and Counsel to the Assistant Attorney General for National Security in the U.S. Department of Justice. Mr. Jaffer is testifying before the Senate Banking Committee in his personal and individual capacity and is not testifying on behalf of any organization or entity, including but not limited to any current or former employer.

² Significant portions of this testimony have been drawn in whole or in part from an NSI Decision Memo entitled *Addressing the National Security Threat of Chinese Technological Innovation* by Jamil N. Jaffer published in July 2023. Because much of this testimony is drawn directly from that paper, citations to that paper and quotation marks for portions of this testimony drawn from that paper have been omitted, including where significant portions are excerpted verbatim. Professor Jaffer would like to thank Devlin Birnie, Jessica Jones, Harrison McClintock, and Alex Tokie for their excellent research and editing assistance with the original paper. The original paper can be found at: <https://nationalecurity.gmu.edu/addressing-the-national-security-threat-of-chinese-technological-innovation-2/>.

II. The Threat from the People's Republic of China and its Relationship to Technological Innovation and Emerging Technologies

The defining national security challenge facing the United States today is threat posed by a rising China, a nation that not only oppresses its own people, but which also seeks to expand that repression beyond its borders, both within its own region as well as across the globe. One need only look at the PRC's treatment of Muslim Uyghurs in the Xinjiang region—which two successive U.S. administrations have determined constitutes genocide and crimes against humanity³—its repression of dissent in Hong Kong and Tibet, its military and economic threats against Taiwan, its belligerent actions against other U.S. allies in the region, including the Philippines, its export of surveillance and other repressive technologies across the globe, its theft of core intellectual property from private sector companies in the United States and allied nations, its growing cyber infiltrations of U.S. and allied critical infrastructure, its attempts to consolidate its control over key critical minerals and strategic metals and to withhold access to them, its belligerent posture to America and allied national security priorities in a wide range of regions, and its extortion of dozens of countries under the Belt and Road Initiative (BRI), to see just a few examples of the massive and growing threat that the China poses to the United States, our allies, and a host of other nations across the globe. And this doesn't even account for China's growing political, economic, and military relationships with other global repressors like Russia, Iran, and North Korea.

At the core of this national security threat that the PRC poses to the United States, as well as our global competition with China for supremacy—whether in the economic, political, military, or social spheres—is technological innovation, including access to and control over critical emerging technologies, particularly artificial intelligence capabilities.⁴ In recent decades, the PRC has made

³ See Michael R. Pompeo, *Press Statement: Determination of the Secretary of State on Atrocities in Xinjiang*, United States Department of State (Jan. 19, 2021), available online at <<https://2017-2021.state.gov/determination-of-the-secretary-of-state-on-atrocities-in-xinjiang/>> (“After careful examination of the available facts, I have determined that since at least March 2017, the People’s Republic of China (PRC), under the direction and control of the Chinese Communist Party (CCP), has committed crimes against humanity against the predominantly Muslim Uyghurs and other members of ethnic and religious minority groups in Xinjiang ... In addition, after careful examination of the available facts, I have determined that the PRC, under the direction and control of the CCP, has committed genocide against the predominantly Muslim Uyghurs and other ethnic and religious minority groups in Xinjiang. I believe this genocide is ongoing, and that we are witnessing the systematic attempt to destroy Uyghurs by the Chinese party-state.”); see also, e.g., United States Department of State, *2021 Country Reports on Human Rights Practices: China (Includes Hong Kong, Macau, and Tibet)* (Apr. 12, 2022), available online at <<https://www.state.gov/reports/2021-country-reports-on-human-rights-practices/china/>> (“Genocide and crimes against humanity occurred during the year against predominantly Muslim Uyghurs and members of other ethnic and religious minority groups in Xinjiang.”)

⁴ See, e.g., The White House, *National Security Strategy* (Oct. 2022), at 23, available online at <<https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf>> (“The PRC is the only competitor with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to do it ... It is using its technological capacity and increasing influence over international institutions to create more permissive conditions for its own authoritarian model, and to mold global technology use and norms to privilege its interests and values.”); Xi Jinping, *Speech to Members of the Chinese Academy of Sciences, the Chinese Academy of Engineering, and the National Congress of China Association for Science and Technology* (May 28, 2021) (translated by Zichen Wang), available online at <<https://www.pekingology.com/p/xi-jinpings-speech-on-science-and-s-t/>> (“[S]cientific and

aggressive moves to build its own technological innovation base and now seeks to expand its capabilities.⁵ Much of this effort by the PRC initially began by actively seeking to dominate the manufacturing market for technology goods, producing equipment at costs well below those achievable in most other economies.⁶ This was achieved, in significant part, by exploiting the PRC's theft of U.S. intellectual property at industrial scale—referred to as the greatest transfer of wealth in modern human history⁷—which was then leveraged to create an entire industry of state-owned and state-influenced enterprises that, when combined today, generate a tremendous amount of the technology products and capabilities sold around the globe, including producing goods on behalf of a number of highly innovative American companies, competing with others, and replacing or coopting yet others in the global market.⁸ Worse still, the PRC is now going well

technological innovation has become the main battlefield of the international strategic game, and the competition around the commanding heights of science and technology is unprecedentedly fierce.”).

⁵ See, e.g., Tarun Chhabra, et. al, *Executive Summary – Global China: Assessing China's Growing Role in the World*, Brookings Institution (Apr. 2020), available online at <<https://www.brookings.edu/articles/global-china-technology/>> (“China's rapid technological advances are playing a leading role in contemporary geopolitical competition... While the U.S. has maintained its position as the technologically dominant power for decades, China has made enormous investments and implemented policies that have contributed significantly to its economic growth, military capability, and global influence. In some areas, China has eclipsed, or is on the verge of eclipsing, the United States — particularly in the rapid deployment of certain technologies.”); Bloomberg News, *How China Aims to Counter US 'Containment' Efforts in Tech*, Washington Post (Mar. 30, 2023), available online at <https://www.washingtonpost.com/business/2023/03/30/explainer-how-china-aims-to-counter-us-containment-efforts-in-tech/ea71f0c-cfd-11ed-8907-156f0390d081_story.html> (“Chinese President Xi Jinping... and his new lieutenants are deploying what they call a “whole nation” system: marshaling resources and companies from across the country — and trillions of dollars — to drive research and development.”).

⁶ See Wayne M. Morrison, *China's Economic Rise: History, Trends, Challenges, and Implications for the United States*, Congressional Research Service (June 25, 2019), at 23, available online at <<https://crsreports.congress.gov/product/pdf/RL/RL33534>> (“China's abundance of low-cost labor has made it internationally competitive in many low-cost, labor-intensive manufactures. As a result, manufactured products constitute a significant share of China's trade. A substantial amount of China's imports is comprised of parts and components that are assembled into finished products, such as consumer electronic products and computers, and then exported.”)

⁷ See, e.g., Keith B. Alexander, *Prepared Statement of GEN (Ret) Keith B. Alexander, A Borderless Battle: Defending Against Cyber Threats*, House Committee on Homeland Security (Mar. 22, 2017), available online at <<https://www.congress.gov/115/meeting/house/105741/witnesses/HHRG-115-HM00-Wstate-AlexanderK-20170322.pdf>> (“[T]he ongoing theft of intellectual property from American companies... continues to represent the greatest transfer of wealth in human history.”); Senator Carl Levin, *Opening Statement of Chairman Carl Levin in Hearing to Receive Testimony on U.S. Strategic Command and U.S. Cyber Command in Review of the Defense Authorization Request for Fiscal Year 2013 and the Future Years Defense Program*, Senate Armed Services Committee (Mar. 27, 2012), at 3, available online at <<https://www.armed-services.senate.gov/imo/media/doc/12-19%20-%20203-27-12.pdf>> (“General Alexander has stated that the relentless industrial espionage being waged against U.S. industry and Government chiefly by China constitute “the largest transfer of wealth in history.”).

⁸ See, e.g., Special Competitive Studies Project, *Generative AI: The Future of Innovation Power* (Oct. 2023), at 3 & n.6 (collecting sources), 10-12 and 23, available online at <<https://www.scspp.ai/wp-content/uploads/2023/10/economy.pdf>>; Brady Helwig, et al., *National Action Plan for Advanced Compute & Microelectronics*, Special Competitive Studies Project (Nov. 2023), at 8-9, 13, 32, and 39, available online at <<https://www.scspp.ai/wp-content/uploads/2023/11/National-Action-Plan-for-U.S.-Advantage-in-Advanced-Compute-and-Microelectronics.pdf>>; see also, e.g., John Miller & Sacha Wunsch-Vincent, *High-Tech Trade*

beyond manufacturing-at-scale and is creating innovation on top of this stolen IP and securing its access to data, as it recognizes that whichever nation dominates the technology revolution—particularly in emerging technology areas like quantum computing, biotechnology, and artificial intelligence (the latter of which is particularly data reliant)—will likely also win the larger geopolitical competition.⁹

A key aspect of the PRC’s effort to lead in the technology domain is its centralized planning efforts that have been in place for well over a decade, including its Made in China 2025 line of effort (“PRC 2025”), a “broad set of industrial plans that aim to boost competitiveness by advancing China’s position in the global manufacturing value chain, ‘leapfrogging’ into emerging technologies, and reducing reliance on foreign firms.”¹⁰ This effort aims to enable China to “make major technology breakthroughs, lead innovation in specific industries, and set global standards” by 2035 and “[l]ead global manufacturing and innovation with a competitive position in advanced technology and industrial systems” by 2049, with key areas of focus including next generation IT and telecommunications capabilities, high performance computing, advanced robotics, and artificial intelligence.¹¹ And in the critically important AI domain, China released a plan back in 2017—long before the public advent of highly-capable generative AI in 2022 and even well prior to the enactment of the U.S. National AI Initiative Act of 2020—to “lead the world in AI by 2030.”¹² While ostensibly emphasizing domestic development in these national plans, it is clear that the PRC plans to continue to rely on the “acquisition, absorption, and adaptation of foreign technology by PRC entities that recast these capabilities as their own,”¹³ and then build upon these stolen technologies to create additional innovation.

China’s acquisition of U.S. and allied emerging technology takes place through a range of vectors: (1) outright theft of intellectual property;¹⁴ (2) forced technology transfer from companies seeking to enter the Chinese market;¹⁵ (3) requiring new market entrants to establish joint ventures with

Rebounded Strongly in the Second Half of 2020, with New Asian Exporters Benefiting (Mar. 15, 2021), available online at <https://www.wipo.int/pressroom/en/news/2021/news_0001.html>.

⁹ *Id.*

¹⁰ See Karen M. Sutter, “Made in China 2025” Industrial Policies: Issues for Congress, Congressional Research Service (Mar. 10, 2023), at 1, available online at <<https://crsreports.congress.gov/product/pdf/IF/IF10964>>.

¹¹ *Id.*

¹² See SCSP, *Generative AI*, *supra* at n. 8, at 3 & n. 6.

¹³ *Id.*

¹⁴ See, e.g., Office of the U.S. Trade Representative, *2023 Special 301 Report*, Executive Office of the President, The White House (Apr. 2023), at 9, 22-23, 45-47, available online at <<https://ustr.gov/sites/default/files/2023-04/2023Special301Report.pdf>>; see also Keith B. Alexander and Jamil N. Jaffer, *China Is Waging Economic War on America. The Pandemic Is an Opportunity to Turn the Fight Around*, *Barron’s* (August 4, 2020), available online at <<https://www.barrons.com/articles/china-is-waging-cyber-enabled-economic-war-on-the-u-s-how-to-fight-back-51596587400>>.

¹⁵ *Id.*

PRC companies;¹⁶ (4) requiring sensitive IP to be kept in China;¹⁷ (5) tax incentives to get production and R&D moved to China;¹⁸ (6) acquisition of American and allied companies with sensitive technologies directly or through bankruptcy proceedings;¹⁹ (7) corporate and government partnerships with U.S. companies, universities, and individual experts or academics, including through PRC talent programs and educational pipeline work;²⁰ and (8) joining and setting the agenda for international standards setting bodies.²¹ And China has doubled down on these efforts, making clear that it will continue to exploit its foreign research connections, use domestic regulatory measures and influence abroad in areas like antitrust, IP, and international standards,²² as well as make massive investments into key emerging technology areas, including quantum computing, robotics, artificial intelligence, and cybersecurity,²³ both directly and by offering low-interest and no-interest loans and massive state-driven subsidies—totaling well-over a trillion

¹⁶ See, e.g., Sean O'Connor, *How Chinese Companies Facilitate Technology Transfer from the United States*, U.S.-China Economic Security Review Commission, at 7 (May 6, 2019), available online at <<https://www.uscc.gov/sites/default/files/Research/HowChineseCompaniesFacilitateTechTransferfromtheUS.pdf>>

¹⁷ *Id.* at 8.

¹⁸ See, e.g., Erica York, et al., *Comparing the Corporate Tax System in the U.S. & China*, Tax Foundation, at 4 (May 2022), available online at <<https://files.taxfoundation.org/20220502152914/Comparing-the-Corporate-Tax-Systems-in-the-United-States-and-China.pdf>>.

¹⁹ See, e.g., Cory Bennet & Bryan Bender, *How China Acquires 'The Crown Jewels' of U.S. Technology*, Politico (May 22, 2018), available online at <<https://www.politico.com/story/2018/05/22/china-us-tech-companies-cfius-57241>>; Camille A. Stewart, *Full Court Press: Preventing Foreign Adversaries from Exfiltrating National Security Technologies Through Bankruptcy Proceedings*, 10 J. Nat'l Security L. & Pol'y 277, 279-82 (2019).

²⁰ See, e.g., Alison Snyder, *China Talent Program Increased Young Scientists' Productivity, Study Says*, Axios (Jan. 10, 2023), available online at <<https://www.axios.com/2023/01/10/china-funding-young-scientists-productivity>>; see also Emily S. Weinstein, *Chinese Talent Program Tracker*, Center for Security and Emerging Technology, Georgetown University (Nov. 2020), available online at <<https://cset.georgetown.edu/publication/chinese-talent-program-tracker>>; Federal Bureau of Investigation, *The China Threat - Chinese Talent Plans Encourage Trade Secret Theft, Economic Espionage*, Federal Bureau of Investigation, available online at <<https://www.fbi.gov/investigate/counterintelligence/the-china-threat/chinese-talent-plans>>.

²¹ See, e.g., Arjun Gargayas, *China's '2035 Standards' Quest to Dominate Global Standard-Setting*, Hinrich Foundation (Feb. 21, 2023), available online at <<https://www.hinrichfoundation.com/research/article/trade-and-geopolitics/china-2035-standards-project-restructure-global-economy/>>.

²² See Sutter, *Made in China 2025*, supra n. 10 at 2 ("Similarly, the FYP calls for an expanded use of antitrust, IP, and standards tools—in China and extraterritorially—to set market terms and promote the export of MIC2025 goods and services now coming to market. The FYP also emphasizes the value of China's foreign research ties in developing China's own competencies in a range of MIC2025 technology areas.").

²³ See *id.*

dollars—to enable its companies to compete more favorably in global markets,²⁴ while also using board seats influence corporate decision-making.²⁵

We know also that China is actively working to get other nations to put Chinese national champion technology capabilities—from telecoms to chips—at the heart of their networks,²⁶ and that it continues to build out its STEM workforce, proactively recruiting leading STEM players from around the world,²⁷ and, having already passed the U.S. in the number of annual Ph.Ds awarded many years back, some estimate that the PRC may annually graduate nearly double the number of STEM Ph.Ds as the U.S. in the near future.²⁸ All of these efforts are also buttressed by China's longer-term efforts to secure its access to critical minerals, strategic metals, and energy resources, from production to processing,²⁹ and its parallel efforts to exclude U.S. and allied partners from access to such resources, all of which are critical to our technological and industrial innovation base.³⁰

²⁴ See, e.g., Jill C. Gallagher, *U.S. Restrictions on Huawei Technologies: National Security, Foreign Policy, and Economic Interests*, Congressional Research Service (Jan. 5, 2022), at 7-8, available online at <<https://crsreports.congress.gov/product/pdf/R/R47012/2>> (describing how “[n]ational champions [in China], including Huawei, received preferential policy treatment, access to low-cost financing, R&D funding, and tax benefits”); see also, e.g., Ann Harrison, et al., *Can a Tiger Change Its Stripes? Reform of Chinese State-Owned Enterprises in the Penumbra of the State*, NBER Working Paper No. 25475 (Jan. 2019), at 24, available online at <https://www.nber.org/system/files/working_papers/w25475/w25475.pdf> (noting that former Chinese state-owned enterprises, like SOEs themselves, generally “retain ready access to large loans, concessionary interest rates, and outright subsidies”).

²⁵ See, e.g., Scott Livingston, *The New Challenge of Communist Corporate Governance*, Center for Strategic & International Studies (Jan. 2021), at 2-4, available online at <https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210114_Livingston_New_Challenge.pdf>.

²⁶ See Joshua Kurlantzick, *Assessing China's Digital Silk Road Initiative*, Council on Foreign Relations (Dec. 18, 2020), available online at <<https://www.cfr.org/china-digital-silk-road>>; Chang Che and John Liu, ‘De-Americanize’: How China Is Remaking Its Chip Business, *New York Times* (May 11, 2023), available online at <<https://www.nytimes.com/2023/05/11/technology/china-us-chip-controls.html>>.

²⁷ See, e.g., Eric Schmidt, *To Compete With China on Tech, America Needs to Fix Its Immigration System*, *Foreign Affairs* (May 16, 2023), available online at <<https://www.foreignaffairs.com/united-states/eric-schmidt-compete-china-tech-america-needs-fix-its-immigration-system>> (“While the United States’ dysfunctional system increasingly deters the world’s top scientists, researchers, and entrepreneurs, other countries are proactively recruiting them. China is particularly active in doing so, with direction coming from the very top.”).

²⁸ See, e.g., Karin Fischer, *China Outpaces U.S. in STEM*, Georgetown Center for Security and Emerging Technology, *Latitudes* (Aug. 9, 2021), available online at <<https://cset.georgetown.edu/article/china-outpaces-u-s-in-stem/>>. (“China could graduate nearly twice as many STEM PhDs as the United States by 2025... China overtook the U.S. in PhD production in 2007 and has steadily increased its lead ever since.”).

²⁹ See Jane Nakano, *The Geopolitics of Critical Minerals Supply Chains*, Center for Strategic & International Studies, at 5 (March 2021), available online at <https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210311_Nakano_Critical_Minerals.pdf>.

³⁰ See, e.g., Arjun Kharpal, *What are Gallium and Germanium? China Curbs Exports of Metals Critical to Chips and Other Tech*, *CNBC* (July 4, 2023), available online at <<https://www.cnbc.com/2023/07/04/what-are-gallium-and-germanium-china-curbs-exports-of-metals-for-tech.html>>; see also Mai Nguyen, *China's Rare Earths Dominance in Focus After it Limits Germanium & Gallium Exports*, *Reuters* (July 5, 2023), available online at <<https://www.reuters.com/markets/commodities/chinas-rare-earths-dominance-focus-after-mineral-export-curbs-2023-07-05/>>.

III. The Need for a Strong U.S. Government Response to the Emerging Technology Threat from China

The United States has thus far used a variety of tools to push back on unfair PRC technology practices, including IP theft and forced technology transfers,³¹ “ramped up law enforcement to counter China’s theft of U.S. IP, restricted certain PRC firms from U.S. infrastructure, started to scrutinize China’s role in federally funded research,”³² and focused efforts on stopping the PRC’s exploitation of U.S. technology researchers in academia and industry.³³ The Administration has also sought to work both independently and with our allies, like the EU, to limit technology transfers to China in critical areas like aerospace technologies³⁴ and semiconductors,³⁵ and has begun the process of identifying categories of outbound investments that ought be reported or restricted.³⁶ Congress, for its part, has provided for additional review of Chinese transactions in the United States,³⁷ enhanced American export control laws,³⁸ and made major new R&D and production investments and commitments to fund new efforts in areas like semiconductors.³⁹

³¹ See, e.g., Office of the U.S. Trade Representative, *Section 301 Investigation Fact Sheet*, Executive Office of the President, The White House (June 2018), available online at <<https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2018/june/section-301-investigation-fact-sheet>> (noting that the Trump Administration invoked Section 301 authorities and imposed tariffs on most imports from China in response to findings that China’s IP policies harmed U.S. stakeholders); see also Sutter, *Made in China 2025*, *supra* n. 10 at 2 (noting that a January 2020 bilateral economic and trade agreement resulted in some IP and technology transfer commitments by China but left most U.S. concerns unresolved).

³² Sutter, *Made in China 2025*, *supra* n. 10 at 2; see also, e.g., Ana Swanson, *Trump’s Trade War With China is Officially Underway*, New York Times (July 5, 2018), available online at <<https://www.nytimes.com/2018/07/05/business/china-us-trade-war-trump-tariffs.html>>.

³³ See, e.g., Snyder, *China Talent Program*, *supra* n. 20.

³⁴ See Sutter, *Made in China 2025*, *supra* n. 10 at 2.

³⁵ See, e.g., Tim Kelly, et al., *Japan, Netherlands to Join U.S. in Restricting Chip Equipment Exports to China*, Bloomberg Reports, Reuters (Jan. 27, 2023), available online at <<https://www.reuters.com/technology/japan-netherlands-join-us-china-chip-controls-bloomberg-2023-01-27/>>.

³⁶ See The White House, *Executive Order on Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern* (Aug. 9, 2023), available online at <<https://www.whitehouse.gov/briefing-room/presidential-actions/2023/08/09/executive-order-on-addressing-united-states-investments-in-certain-national-security-technologies-and-products-in-countries-of-concern/>>.

³⁷ See John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, §§ 1701-28 (2018) (Foreign Investment Risk Review Modernization Act of 2018).

³⁸ See, e.g., Michael Geffroy and Andy Keiser, *NSI Policy Brief: Restricting U.S. Outbound Investment to Targeted Chinese Sectors*, National Security Institute, George Mason University Scalia Law School (May 2023), available online at <<https://nationalsecurity.gmu.edu/restricting-u-s-outbound-investment-to-targeted-chinese-sectors/>> (discussing export control authorities and the importance of stepping cautiously).

³⁹ See CHIPS Act of 2022, Pub. L. No. 117-167, § 103 (2022).

critical minerals,⁴⁰ basic science research,⁴¹ OPEN-RAN,⁴² and other emerging technologies under the CHIPS and Science Act.⁴³

At the same time, significantly more needs to be done if we are to successfully and effectively take on the threat that China poses to our economic and national security.

First, when it comes to government action, there is no question that the United States government needs to expand its efforts and provide the requisite funding necessary to support key basic science research, including providing appropriations for some of the key programs authorized in the CHIPS and Science Act,⁴⁴ as this type of funding has historically supported major breakthroughs in areas like biosecurity, high-performance and accelerated computing, quantum computing, and artificial intelligence, to name just a few.⁴⁵ For those concerned that such funding might involve the government too directly in private markets, it is worth noting that the kind of core capability development driven by basic science research is often well removed from the goods that actually enter the market, and government funding has long played a central role in providing support for the kind innovation that is fundamental to our security interests, from defense technology to telecommunications. Such early-stage base funding is particularly important when the applied business uses cases may not be obvious enough to attract core private funding.⁴⁶

⁴⁰ See, e.g., Infrastructure Investment and Jobs Act, Pub. L. No. 117-58, §§ 40206, 40210 (2021).

⁴¹ See, e.g., Pub. L. No. 117-167, §§ 10102-103, 10105-113, 10348-362 (2022).

⁴² See CHIPS Act, *supra* n. 39, § 106; see also National Telecommunications and Information Administration, *Wireless Innovation Fund Notice of Funding Opportunity*, U.S. Dept. of Commerce (Apr. 12, 2023), available online at <<https://www.ntia.gov/issues/innovation-fund/notice-of-funding-opportunity>>.

⁴³ See, e.g., Pub. L. No. 117-167, §§ 10104, 10230, 10374 (2022).

⁴⁴ See, e.g., Pub. L. No. 117-167, §§ 10101-114 (basic science); §§ 10221-235 (basic science); §§ 10311-321 (STEM education & workforce) & §§ 10501-526 (STEM education & workforce).

⁴⁵ See James Manyika et al., *Innovation and National Security - Keeping Our Edge*, Council on Foreign Relations (Sep. 2019), at 2, 19, available online at <https://www.cfr.org/report/keeping-our-edge/pdf/TFR_Innovation_Strategy.pdf> (“Federally supported R&D had a dramatic impact on U.S. competitiveness and national security. According to a 2019 study, starting in the 2010s nearly one-third of patented U.S. inventions relied on federally funded science []. Touch screens, the Global Positioning System (GPS), and internet technologies central to the smartphone are all products of Defense Department research. . . . Between 1988 and 2010, \$3.8 billion of federal investment in genomic research generated an economic impact of \$796 billion and created 310,000 jobs. A new wave of support for basic research could have similar economic and military benefits.”); see also Jamie Gaida et al., *ASPI’s Critical Technology Tracker: The Global Race for Future Power*, Australian Strategic Policy Institute (Feb. 2023), at 1, available online at <https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2023-03/ASPIs%20Critical%20Technology%20Tracker_0.pdf> (noting that “China’s global lead extends to 37 out of 44 technologies that ASPI is now tracking, covering a range of crucial technology fields spanning defence, space, robotics, energy, the environment, biotechnology, artificial intelligence (AI), advanced materials and key quantum technology areas”).

⁴⁶ See *id.* at 21 (“Public spending on basic science drives discoveries that would have been too big and risky for a private company to undertake. In effect, federal investment funds R&D with national economic, strategic, and social returns, while private sector R&D is motivated by commercial returns. Moreover, public R&D creates spillovers that benefit the entire economy and incentivize greater R&D funding in the private sector.”)

Second, to ensure the U.S. is able to effectively compete with China, the government should provide significant tax and other economic incentive to startups, as well as other companies that can rapidly and massively scale up (therefore effectively compete with Chinese national champions)—and remove existing regulatory and other barriers—for increased private basic and applied R&D investment in critical emerging technology areas like: (1) high-performance and accelerated computing; (2) quantum technology; (3) cloud and edge computing capabilities, particularly for the warfighter; (4) AI/ML capabilities, including generative AI, as well as capabilities to enhance the trust, safety, and security of AI-enabled systems; (5) design and production, in the United States and allied nations, of both commodity and bleeding-edge semiconductors, particularly for artificial intelligence and other critical applications; (6) production and processing, in the United States and allied nations, of critical minerals necessary for national security and technology applications; and (7) enhanced cybersecurity efforts and protection of intellectual property.

Third, while incentivizing such investments, U.S. and allied governments (across both the legislative and executive branches), should also ensure that they are not actively taking action—whether through overregulation or otherwise—that would undermine the ability of key American and allied companies to scale their capabilities, disincentivize innovation and investment in critical emerging technologies, or take advantage of new innovations in a manner that allows us to actively stay ahead of the PRC. This means, for example, not adopting significant new regulatory or administrative policies—including adopting new laws or gerrymandering enforcement efforts to focus on a narrow set of technology leaders—that would undermine the ability of the United States to effectively compete on a global scale and thereby undermine our economic and national security. This also includes, for example, modifying longstanding and highly effective antitrust laws to intentionally target some of the most innovative and scalable companies in the AI space,⁴⁷ particularly given that there is no clear reason to believe existing law can't address any legitimate concerns.⁴⁸ Indeed, requiring successful American technology companies to give foreign competitors deep access to their hardware and software, bypassing traditional security controls, could create a massive nightmare and undermine our economic and national security.⁴⁹ Ensuring we have the right incentives in place also means recognizing that overaggressive or selective

⁴⁷ See, e.g., American Innovation and Choice Online Act, S.2992, 117th Cong. (2021); Open App Markets Act, S.2710, 117th Cong. (2021); Bill Evanina & Jamil N. Jaffer, *Kneecapping U.S. Tech Companies Is a Recipe for Economic Disaster*, Barron's (June 17, 2022), available online at <<https://www.barrons.com/articles/kneecapping-u-s-tech-firms-is-a-recipe-for-economic-disaster-51655480902>> (“Conservatives are often worried—sometimes for good reason—that certain social or mainstream media companies might actively seek to suppress or quiet conservative voices. On the liberal side, there are a range of legitimate concerns with technology companies, including the displacement of traditional labor in the new gig economy... Yet rather than tackling these concerns directly by going after the specific behaviors or actions that trouble ordinary Americans, politicians in Washington have chosen instead to vilify some of our most successful companies and to go after them economically.”); see also David R. Henderson, *A Populist Attack On Big Tech*, The Hoover Institution (Mar. 3, 2022), available online at <<https://www.hoover.org/research/populist-attack-big-tech-0>>; Klon Kitchen & Jamil Jaffer, *The American Innovation & Choice Online Act Is A Mistake*, The Kitchen Sync (Jan. 19, 2022), available online at <<https://www.thekitchensync.tech/p/the-american-innovation-and-choice>>.

⁴⁸ See Henderson, *A Populist Attack on Big Tech*, *supra* n. 47; Evanina & Jaffer, *Kneecapping U.S. Tech Companies*, *supra* n. 47.

⁴⁹ See Kitchen & Jaffer, *The American Innovation & Choice Online Act*, *supra* n. 47; Evanina & Jaffer, *Kneecapping U.S. Tech Companies*, *supra* n. 47.

enforcement of existing laws in other domains—including the environmental and sanctions context—can undermine larger innovation policy efforts.⁵⁰ To the extent the government has discretion in how the laws or regulatory policies are to be enforced, it should be done in an evenhanded manner and should account for the innovation impacts of such enforcement as well.

Fourth, it is critical that the United States both create a STEM-capable workforce here in the United States. In doing so, Congress funding some of the key workforce-related programs authorized in the CHIPS and Science Act,⁵¹ and should consider redirecting existing resources and providing new resources to states in the form of block grants,⁵² and encouraging them to deploy these grants through public schools, public charter schools (some of which have highly innovative curricula in the technology domain),⁵³ and, as appropriate, private institutions. This effort must be partnered with programs that provide incentives innovators and entrepreneurs to stay, develop new technology, and build businesses in the United States over the long-term, including tax benefits for building new startups in the U.S. and hiring American workers to develop code. Of course, this is a long-term plan, and the fact of the matter is that we need to fill the significant existing technology worker gap now.⁵⁴ To do so, we must fundamentally reform our broken immigration

⁵⁰ See, e.g., Phillip Singerman and Alexander Kersten, *Implementing CHIPS: The NEPA Permitting Challenge*, Center for Strategic and International Studies (May 1, 2023), available online at <https://www.csis.org/analysis/implementing-chips-nepa-permitting-challenge> (“[F]ederal funding under the CHIPS Act triggers the federal NEPA review process... This has raised fears that complying with the NEPA review could stall projects for over two years and cost the firms billions, undermining the policy imperatives of CHIPS... Currently, there is uncertainty about how these rules will apply to the construction of semiconductor fabs stimulated by the CHIPS Act... Further, the Council on Environmental Quality (CEQ) claims that between 2013 and 2018 Environmental Impact Statements took an average of 4.5 years to complete. This implies that any fab that is obligated to generate an Environmental Impact Statement would likely face significant delays. Some estimates put delay costs for large infrastructure projects as high as 5 percent a year, meaning, for example, that Intel’s planned \$20 billion investment in Ohio could encounter about \$1 billion in extra expenses for every year delayed.”).

⁵¹ See McKinsey & Co., *The CHIPS and Science Act: Here’s What’s in It* (Oct. 4, 2022), available online at <https://www.mckinsey.com/industries/public-sector/our-insights/the-chips-and-science-act-heres-whats-in-it> (noting that the CHIPS and Science Act “authorizes (but does not yet appropriate) \$174 billion over the next five years to various federal science agencies to invest in STEM, workforce development, and R&D, with some \$80 billion earmarked for the National Science Foundation”).

⁵² Cf. National Science Teachers Association, *FACT SHEET: Title IV, Part A of ESSA: Student Support and Academic Enrichment Grants and Science/STEM Education*, available online at <https://static.nsta.org/pdfs/ESSATitleIV-ScienceSTEMFactSheet.pdf> (describing the \$1.65 billion Student Support and Academic Enrichment block grant program under The Every Student Succeeds Act (ESSA) enacted in 2014, which consolidated the Math and Science Partnership Grants, which is described as “the largest single program at the Department of Education devoted exclusively to science/STEM-related classroom purposes,” having “received \$152.7M in FY2016 before it was eliminated”).

⁵³ See, e.g., Digital Pioneers Academy, *Our Academic Model*, available online at <https://www.digitalpioneersacademy.org/enroll/academic-model> (describing the D.C. charter school’s unique model of two teachers per classroom and requiring one hour of computer science per day for students at all grade levels); Digital Pioneers Academy, *Computer Science Model*, available online at <https://www.digitalpioneersacademy.org/enroll/csmodel> (describing the Digital Pioneer’s curriculum as requiring students to “[t]ake and pass the Computer Science Advanced Placement exam in 10th grade [and] [m]aster two programming languages by 12th grade.”).

⁵⁴ See Schmidt, *To Compete with China on Tech*, *supra* n. 27 (“According to current projections, U.S. semiconductor companies will have 300,000 unfilled vacancies for skilled engineers by 2030. Targeting, training,

system to ensure that we are recruiting and retaining the best and brightest minds the world has to offer. Our current immigration system makes little sense, in that it allows a wide range of undergraduate and graduate students to benefit from our world-class higher education system, but then—with exception of the small number that are able to obtain H-1B visas or otherwise stay in the United States—forces them to return home and build their businesses abroad.⁵⁵ Indeed, this poorly thought-out policy actually forces American companies to hire high-skilled workers abroad and deprives our own economy of the benefits of their employment here, including the tax revenues and spending of these high-skilled, high-wage workers.⁵⁶ There is no reason why—other than the obvious political challenges—the United States couldn't create a much more sensible immigration system that prioritizes those with the key skills we need and provides for a stringent pre-admission vetting to address potential IP theft and foreign intelligence concerns. Such a system could provide both a path to work and permanent residency for those that build successful businesses here. Such a system would stand in sharp contrast to the current lottery system which provides a level of randomness that makes little, if any, sense. Examples of ideas that might move us in the right direction can be found in a recent CSIS report,⁵⁷ and in more limited form in earlier versions of the CHIPS and Science Act, as well as in other proposals that have garnered bipartisan support.⁵⁸ The ongoing failure to address the very real problem created by our immigration system today, as well as the long-term challenge in our educational system when it comes to STEM education is, without a doubt, creating significant national security risk at a time when the U.S. can least afford it, particularly as our adversaries look to take advantage.

Fifth, the government could do more to identify, target, and limit strategic Chinese investment in the United States. Our current laws remain challenged in addressing the threat from China, because they apply in a “country-agnostic [manner], treating investment from foreign adversary countries like the PRC the same as that of any other country” and also don't provide jurisdiction

and recruiting hundreds of thousands of U.S. citizens will be impossible in such a compressed time frame. The only way to meet this demand is to recruit many more skilled workers from abroad.”).

⁵⁵ *Id.* (“[T]he United States has long relied on its companies and universities to attract the world's best and brightest. Brilliant engineers from all around the world helped me turn Google into a world-leading technology company. But this did not happen because of the U.S. immigration system. It happened in spite of it.”).

⁵⁶ See Paayal Zaveri, *America's Immigration System is a Nightmare & it's Forcing Tech Companies to Move Jobs Outside of the Country*, Business Insider (Mar. 14, 2023), available online at <<https://www.businessinsider.com/us-tech-firms-offshoring-immigration-labor-shortage-issues-remote-work-2023-3>> (“[T]he difficulties in bringing immigrants into the US is pushing companies to instead hire them to work in other countries. That, in turn, is encouraging those same companies to open branch offices in other countries and recruit there, staffing them with people who might otherwise have come to the US to work[.]”).

⁵⁷ See William Alan Reinsch & Thibault Denamiel, *Immigration Policy's Role in Bolstering the U.S. Technology Edge*, Center for Strategic & International Studs. (Feb. 6, 2023), available online at <<https://www.csis.org/analysis/immigration-policies-role-bolstering-us-technology-edge>>; see also William R. Kerr & Sari Pekkala Kerr, *Immigration Policy Levers for U.S. Innovation & Startups*, Harvard Business School, Working Paper 20-105 (Apr. 2020), available online at <[https://www.hbs.edu/ris/Publication Files/20-105_aac0d5ae-e6e3-4570-8225-31bce127f693.pdf](https://www.hbs.edu/ris/Publication%20Files/20-105_aac0d5ae-e6e3-4570-8225-31bce127f693.pdf)>.

⁵⁸ See H. Comm. On Rules, H.R. 7900, Amend. 117-54 (July 12, 2022), <https://amendments-rules.house.gov/amendments/LOFGRE_036_xml220705125918927.pdf> (showing an unenacted amendment by Congresswoman Lofgren (CA-18)); see also Reinsch & Denamiel, *Immigration Policy's Role*, *supra* n. 57 (“Last year, there was bipartisan support for making available additional green cards with shorter wait times for STEM Ph.D.'s. Yet ultimately this initiative was stripped from the final National Defense Authorization Act.”).

over certain critical technologies and joint ventures, among other things.⁵⁹ The China Select Committee in the House of Representatives has recently suggested some potential changes to existing laws that are worth taking seriously.⁶⁰

IV. The Critical Role of Private Actors in Emerging Technology Innovation and the Need for Government and Industry to Work Collaboratively to Protect Our National Security

Today, private sector research and development funding represents 70% of all R&D expenditures in the United States,⁶¹ with technology companies leading the way, making up seven of the top ten R&D spenders, including all of the top five.⁶² It is this expenditure on core R&D—along with the ability to rapidly iterate and innovate, enabled by a permissive economic and legal environment, and the availability of significant amounts of venture and growth capital, as well as a highly-skilled workforce—that makes the U.S. the technology innovation hub of the globe.

These capabilities are not only at the heart of America's economic success, they are also a core reason why our national defense capabilities remain relatively unmatched across the globe today. As such, rather than limiting the capabilities of the top R&D investors in the U.S. to continue to make such investments—including the technology companies that are in the top five R&D spenders in the nation—it is precisely this R&D spend that the U.S. government and our allies ought to be encouraging companies to scale up. Likewise, as noted above, to ensure the U.S. remains a leader in innovation and investment, we must keep in place and expand on the kind of economic incentives and regulatory structures that have worked so well thus far, and must avoid the temptation to artificially restrain successful innovators—whether startups or otherwise—in the absence of actual, demonstrable bad behavior.

There is also critical room for private action as well. Free and open societies grounded in economic liberty, like the United States, are the engine that drives technological innovation and the expansion of economic opportunities for people around the globe. The fact of the matter is that financial investors and capital allocators (whether venture capitalists, private equity investors, or their respective limited partners), as well as the entrepreneurs, startups, and established companies building innovative capabilities in critical areas of emerging technologies, all benefit from being

⁵⁹ See, e.g., Select Committee on the Strategic Competition with the Chinese Communist Party, *Reset, Prevent, Build: A Strategy to Win America's Economic Competition with the Chinese Communist Party* (Dec. 12, 2023), at 31-32, available online at <<https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/reset-prevent-build-scc-report.pdf>>.

⁶⁰ *Id.*

⁶¹ See Jamil N. Jaffer, *NSI Backgrounder: The Role of American Technology Sector in Safeguarding U.S. Economic and National Security*, National Security Institute, GMU Scalia Law School (Dec. 2022), at 1 & n. 6, available online at <<https://nationalsecurity.gmu.edu/the-role-of-american-technology-sector-in-safeguarding-u-s-economic-and-national-security/>> (citing John F. Sargent, U.S. Research and Development Funding and Performance: Fact Sheet, Congressional Research Service (Sept. 13, 2022), available online at <<https://crsreports.congress.gov/product/pdf/R/R44307/18>>).

⁶² See *id.* at 1 & n. 5 (citing Prableen Bajpai, *Which Companies Spend the Most in Research and Development (R&D)?*, Nasdaq (June 21, 2021), available online at <<https://www.nasdaq.com/articles/which-companies-spend-the-most-in-research-and-development-rd-2021-06-21>>).

in the United States and key allied countries, particularly because of the economic and political systems that undergird our nations.

As such, it is reasonable to expect that the financial investors, entrepreneurs, and companies that benefit from these advantages, while seeking significant returns for their investors and powerful capabilities for their customers, ought be incentivized to voluntarily take action, consistent with their own investment and corporate mandates and objectives, to invest in innovation and capabilities that support the United States and our allies, including those capabilities that will enhance the collective defense of our nations. This includes actively promoting innovation in key emerging technologies, like artificial intelligence, cloud and edge computing, quantum computing, cybersecurity, and underlying capabilities like critical minerals, semiconductors, high performance and accelerated computing, as well as capabilities that enhance the trust, safety, and security of such technologies. Likewise, such financial investors and companies that work in critical emerging technology areas ought also be incentivized to voluntarily avoid investments and transfer of capabilities or technology to adversary nations. Such efforts undermine American and allied technological advantage and harm our economic and national security, and thus make it harder to protect the very system that permits the innovation and capital allocation that these organizations rely upon in the daily course of their businesses.

Unfortunately, there is evidence that suggests American investors and companies are making significant investments in leading-edge Chinese companies, including in the artificial intelligence arena.⁶³ Indeed, by one metric, U.S. investors “accounted for nearly a fifth of investment deals in Chinese AI/ML companies from 2015 to 2021.”⁶⁴ Countering the PRC’s effort to establish technology supremacy also requires starving the CCP of its economic lifeblood, capital from abroad, particularly in the form of U.S. investment capital which, while perhaps a small relative amount, nonetheless provides a key signaling function to others. Given the alignment of interests, it is reasonable to expect that some of amount of voluntary action might be sufficient to address some of the key challenges in the current investment environment.

To the extent private action alone does not achieve these goals immediately—whether on investment dollars or technology provision—the government ought be cautious not to reach immediately for the regulatory stick. Rather, additional carrots, like the tax and research and

⁶³ See Emily S. Weinstein & Ngor Luong, *U.S. Outbound Investment into Chinese AI Companies*, Georgetown University Center for Security & Emerging Technology (Feb. 2023), at 11-13, available online at <https://cset.georgetown.edu/wp-content/uploads/CSET-U.S.-Outbound-Investment-into-Chinese-AI-Companies.pdf>; see also Alexandra Alper, *U.S. Investors Have Plowed Billions into China’s AI sector, Report Shows*, Reuters (Feb. 1, 2023), available online at <https://www.reuters.com/technology/us-investors-have-plowed-billions-into-chinas-ai-sector-report-shows-2023-02-01/>; Select Committee on Strategic Competition with the Chinese Communist Party, *Letter to Sequoia Capital on its PRC High-Tech Investments, Examine Implications of Announced Split* (Oct. 18, 2023), available online at <https://selectcommitteeontheccp.house.gov/media/letters/letter-sequoia-capital-its-prc-high-tech-investments-examine-implications-announced>.

⁶⁴ See Alper, *U.S. Investors*, *supra* n. 61; see Weinstein & Luong, *U.S. Outbound Investment*, *supra* n. 61, at 11-12 (showing that 167 U.S. investors took part in 401 transactions, or roughly 17% of the investments into Chinese AI companies in the period; those transactions, in total, represented a total \$40.2 billion in investment, or 37% of the total raised by Chinese AI companies in the 6-year period; it is unclear how much of that amount is attributable to U.S. investors).

development incentives noted above, could have some success in achieving governmental objectives, as they help ensure that the interests of all actors are fully aligned. Forcing companies or investors to do things that are against their financial interests simply ensures that rational economic actors will seek ways around such rules, complying with the specific provisions required, but also taking action where law or regulation permits. It is therefore critical that government and industry work together to create the right tax and regulatory incentives to ensure that American and allied companies invest their money here (and in allied nations) to create much-needed capacity and to ensure that we have the skilled workers necessary to build and maintain this capacity. Moreover, where government does need to act to specifically bar certain investment or technology export activity—potentially even by regulation or statute in critical industries at the heart of U.S. national security like high performance computing, semiconductors, critical minerals, cloud computing, artificial intelligence, and quantum computing—clear rules of the road are critical.⁶⁵ Likewise, the government ought be sure to avoid using taxpayer dollars to companies that are spending capital on advanced capabilities in competitor nations or transferring advanced technology to such nations, like the PRC.⁶⁶

This also means the government needs to take action to open new markets and create the right kind of structures that allow and encourage innovative American business to not only sell to or manufacture in nations that are already aligned with the United States, but also to do so with nations that we would like to see increasingly align with us. The government also ought work with industry to ensure that low-cost capital is available for critical emerging technology companies.⁶⁷

Seeking address the national security threat presented by China standing alone—whether as individual nations or as existing blocs like the EU or the African Union—is also simply untenable. It is critical that the U.S. and our allies work hand-in-hand to address these challenges and stave off the depredations of the PRC. We must find a way to make common cause with our longstanding allies in both Europe and in the Indo-Pacific, as well as the Middle East and Africa, and we must avoid allowing nations that are notionally in our allied bloc from shifting their allegiances and policies towards the PRC.⁶⁸

Likewise, as we think about the role of allies and the relationship of our most innovative private sector actors taking advantage of opportunities in the overseas markets, it is critical that we

⁶⁵ See, e.g., China Select Committee, *Reset, Prevent, Build*, *supra* n. 59 at 28-31.

⁶⁶ See 15 U.S.C. § 4652(a)(5)-(6); see also National Inst. for Standards & Technology, *Proposed Rule: Preventing the Improper Use of CHIPS Act Funding*, 88 FR 17439 (Mar. 23, 2023), available online at <<https://www.federalregister.gov/d/2023-05869>>; Various Authors, *Comments on Proposed Rule: Preventing the Improper Use of CHIPS Act Funding*, available online at <<https://www.regulations.gov/docket/NIST-2023-0001/comments>>.

⁶⁷ See Alexander & Jaffer, *China Is Waging Economic War on America*, *supra* n. 14.

⁶⁸ Eric Cheung, *Honduras Establishes Diplomatic Ties with China, Severs Them With Taiwan*, CNN (Mar. 26, 2023), available online at <<https://edition.cnn.com/2023/03/25/asia/honduras-cuts-diplomatic-ties-with-taiwan-intl-link/index.html>>; Enrique Garcia, *Guatemalan Presidential Contender Pitches Closer China Ties*, Reuters (June 28, 2023), available online at <<https://www.reuters.com/world/americas/surprise-guatemalan-presidential-contender-pitches-closer-china-ties-2023-06-27/>>.

discourage our allies from implementing legislation that undermines the ability of American companies to fairly compete.⁶⁹ For example, nations in Europe and the EU itself have sought to enact and implement aggressive regulatory legislation, including the General Data Protection Regulation (GDPR), the Digital Markets Act (DMA), the Digital Services Act (DSA), and the new AI Act, as well as a range of data sovereignty measures, in ways that makes it difficult for American innovation to reach Europe and limit the access of innovative US industry to the European market. Similar challenges have appeared in the Indo-Pacific as well.⁷⁰ The record is clear that these efforts—at least in Europe—are designed not to enhance competition but to limit it.⁷¹ Given this backdrop, it is incumbent upon the Executive Branch to more aggressively press our allies to align efforts across the Atlantic, including amongst Five Eyes nations, and ensure that we are not taking actions that undermine our collective efforts. Moreover, as some advocate for the government to consider similar regulatory or legislative action in the United States,⁷² it is worth noting that it is the very lack of such efforts that have made the United States so innovative as compared to Europe on a range of metrics, including GDP growth,⁷³ the creation of highly

⁶⁹ See, e.g., General Data Protection Regulation, Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU); Single Market For Digital Services (Digital Services Act), Council Regulation 2022/2065, 2022 O.J. (L 277) 1 (EU); Contestable and Fair Markets in the Digital Sector (Digital Markets Act), Council Regulation 2022/1925, 2022 O.J. (L 265) 1 (EU).

⁷⁰ See, e.g., The Digital Personal Data Protection Bill, 2022, §§ 1-30, available online at <https://www.meitv.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022_0.pdf>; Proposed Digital India Act, 2023, available online at <https://www.meitv.gov.in/writereaddata/files/DIA_Presentation_09.03.2023_Final.pdf>; Shivani Bazaz, *Explained: India's Upcoming Digital Competition Act & What is the Debate Around it All About*, CNBC (Jul. 14, 2023), available online at <<https://www.cnbtv18.com/technology/explained--indias-upcoming-digital-competition-act-and-what-is-the-debate-around-it-all-about-17222501.html>>.

⁷¹ See, e.g., Javier Espinoza, *EU Should Focus on Top 5 Tech Companies, Says Leading MEP*, Financial Times (May 31, 2021), available online at <<https://www.ft.com/content/49f3d7f2-30d5-4336-87ad-eea0ee0ecc7b>> (“The EU lawmaker who will steer the EU’s flagship tech regulation through the European parliament has said it should focus on the largest five US tech companies. Andreas Schwab, a German MEP and longtime critic of Google, spoke after France and Germany both called for the EU to be tougher on Big Tech. He said Google, Apple, Amazon, Facebook and Microsoft, were the ‘biggest problems’ for EU competition policy.”); Adam Satariano, *Meta Fined \$1.3 Billion for Violating E.U. Data Privacy Rules*, New York Times (May 22, 2022), available online at <<https://www.nytimes.com/2023/05/22/business/meta-facebook-eu-privacy-fine.html>>; Rep. Darin LaHood, et al., *Bipartisan Letter from 47 Members of the U.S. to President Biden* (June 22, 2023), available online at <<https://lahood.house.gov/cache/files/6/8/681fc5f3-dacf-458e-9096-0943b2bb2d1f685FC0EBDAF0D803FD514345D8FEF91A.final-letter-to-president-biden-on-eu-digital-trade-concerns--june-2023.pdf>> (describing efforts by the EU “to regulate the digital economy in ways that harm American companies and workers” and arguing that “the discriminatory elements of these policies will weaken American competitiveness by unfairly advantaging domestic European firms and inadvertently benefiting Chinese, Russian, and other foreign-owned competitors”).

⁷² See Cecilia Kang, *As Europe Approves New Tech Laws, the U.S. Falls Further Behind*, New York Times (April 22, 2022), available online at <<https://www.nytimes.com/2022/04/22/technology/tech-regulation-europe-us.html>>.

⁷³ See Jan Rybníček, *Innovation in the United States and Europe*, in *Report on the Digital Economy*, Global Antitrust Institute (2020), available online at <<https://gaidigitalreport.com/2020/08/25/innovation-in-the-united-states-and-europe/>> (“The United States also has greater and faster GDP growth than Europe. Although not a perfect metric, it gives some sense of the contributions that innovative firms have brought to the U.S. economy over time.”); International Monetary Fund, GDP Per Capita, Current Prices: U.S. Dollars Per Capita (2023), available online at <<https://www.imf.org/external/datamapper/NGDPDPC@WEO/EU/USA>>.

successful, highly innovative businesses,⁷⁴ and building private companies whose technology innovations have a massive benefit for national and economic security.⁷⁵ Indeed, such measures make little sense at a time when the key threat to our nations collectively, comes not from within the alliance, but from a rising superpower, like China, that is actively hostile to the world order crafted by the alliance. Indeed, there is support amongst the publics in the U.S. and in our allied nations for increased collaboration on technology and security issues with respect China.⁷⁶

V. The Critical Transformative Capability of Artificial Intelligence.

AI has the potential to have a massively transformative effect on human society, raising all boats, creating new innovation and capability, and allowing a broad range of workers to do ordinary tasks significantly more efficiently, while also freeing innovators to create even more productive tools and capabilities.⁷⁷

While much has been written about the potential of AI to cause significant harm, key claims have been so overwrought and lacking in substance as to undermine their own credibility⁷⁸ or have later been determined to be inaccurate.⁷⁹

⁷⁴ See *id.* (“The United States is home to the most innovative companies that span numerous industries. This includes the most successful global tech firms at the forefront of technological change. These companies consistently outspend their European counterparts on research and development, a key indicator of product improvement and development.”); Michael Ringel et al., *The Most Innovative Companies 2020, The Serial Innovation Imperative*, Boston Consulting Group, at 16 (June 2020), available online at <https://web-assets.bcg.com/img-src/BCG-Most-Innovative-Companies-2020-Jun-2020-R-4_tcm9-251007.pdf>.

⁷⁵ See, e.g., Loren Thompson, *Why Reining In Big Tech Could Be Bad News For U.S. National Security*, *Forbes* (July 7, 2022), available online at <<https://www.forbes.com/sites/lorenthompson/2022/07/07/why-breaking-up-big-tech-could-be-bad-news-for-us-national-security/?sh=1e40190d32bd>>; Jaffer, *The Role of American Technology Sector*, *supra* n. 59.

⁷⁶ See American Edge Project, *U.S. and European Views of the Tech Industry* (Sept. 2022), available online at <<https://americanedgeproject.org/wp-content/uploads/2022/09/AEP-US-EU-Survey-Insights-F9.12.22.pdf>>.

⁷⁷ See, e.g., Chris Inglis, et al., *As the U.S. Sprints Ahead on AI, Values Can't Be Left Behind*, *Barron's* (Oct 26, 2023), available online at <<https://www.barrons.com/articles/ai-regulation-nationalization-innovation-security-6d60ba33>> (“”), see also Michael Chui, et al., *Generative AI is Here: How Tools Like ChatGPT Could Change Your Business*, McKinsey & Co. (Dec. 20, 2022), available online at <<https://www.mckinsey.com/capabilities/quantumblack/our-insights/generative-ai-is-here-how-tools-like-chatgpt-could-change-your-business>>; Dany Hajek, et al., *What Is AI and How Will It Change Our Lives? NPR Explains*, (May 25, 2023), available online at <<https://www.npr.org/2023/05/25/117700852/ai-future-dangers-benefits>>.

⁷⁸ See, e.g., Geoffrey Hinton, et al., *Statement on AI Risk: AI Experts and Public Figures Express their Concern About AI Risk*, Center for AI Risk (May 30, 2023), available online at <<https://www.safe.ai/statement-on-ai-risk/open-letter>> (“Mitigating the risk of extinction from AI should be a global priority alongside other societal-scale risks such as pandemics and nuclear war.”); Max Zahn, *AI Leaders Warn the Technology Poses ‘Risk of Extinction’ Like Pandemics and Nuclear War*, ABC News (May 30, 2023), available online at <<https://abcnews.go.com/Technology/ai-leaders-warn-technology-poses-risk-extinction-pandemics/story?id=99690874>>.

⁷⁹ See Will Knight, *Why the Story of an AI Drone Trying to Kill Its Operator Seems So True*, *Wired* (June 8, 2023), available online at <<https://www.wired.com/story/business-fast-forward>>.

The best approach to protecting U.S. economic and national security in the context of AI—a rapidly moving area of technology innovation where a key consideration is ensuring that government regulation does not crush innovation and deprive society of AI’s potentially massive benefits—is one that allows innovation to flourish, stepping cautiously to address legitimate concerns where regulation may be warranted and appropriate, based on traditional considerations like demonstrable market failures.

As such, rather than rushing to broad-based regulation, as the European Parliament is doing with the AI Act,⁸⁰ imposing significant burdens that may not be directly regulatory but are likely to have a regulatory impact,⁸¹ or directly limiting AI capabilities or applications,⁸² the wiser approach, consistent with the American approach to innovation, would be to prioritize the voluntary adoption of industry-driven frameworks, before moving to a more traditional regulatory posture.⁸³ To that end, encouraging those closest to the actual creation of the technology—the companies, innovators, and investors at the cutting-edge of AI—to craft potential frameworks and industry best practices that might guide the trusted, safe, and secure development and implementation of these technologies, is likely the best approach in the near term. Indeed, providing safe harbors for the implementation of industry best practices and compliance with voluntary, industry-led standards might be a good place for Congress and the Administration to start as they consider potential further action.

VI. Conclusion

For at least a half century, if not significantly longer, the United States has been the world’s leading engine of innovation and investment, driving much of the growth and development of the global information infrastructure, including the Internet as we know it today, and developing the leading-edge technologies that are creating the new and novel capabilities of today, like generative artificial intelligence. This innovation engine has benefitted the United States economically, politically, and militarily, and has provided the very capabilities that have cemented the United States as a global superpower. Today, however, the PRC poses a major strategic challenge to America and our allies across the entire economic and national security landscape. There is little chance that standing alone, any one nation or current bloc of nations will successfully be able to confront and beat China when it comes to economics and (soon) military might. Nor will the any government be able to do it without the cooperation of its private sector. Given the centrality of

⁸⁰ Ryan Browne, *Europe Takes Aim at ChatGPT With What Might Soon be the West’s First A.I. Law. Here’s What It Means*, CNBC (May 15, 2023), available online at <<https://www.cnbc.com/2023/05/15/eu-ai-act-europe-takes-aim-at-chatgpt-with-landmark-regulation.html>> (“A key committee of lawmakers in the European Parliament have approved a first-of-its-kind artificial intelligence regulation — making it closer to becoming law. The approval marks a landmark development in the race among authorities to get a handle on AI, which is evolving with breakneck speed.”).

⁸¹ See The White House, Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

⁸² See *Europe Takes Aim*, *supra* n. 77 (“The AI Act categorizes applications of AI into four levels of risk: unacceptable risk, high risk, limited risk and minimal or no risk. Unacceptable risk applications are banned by default and cannot be deployed in the bloc.”)

⁸³ Cf. *Framework for Improving Critical Infrastructure Cybersecurity*, National Institute of Standards & Technology (Apr. 16, 2018), available online at <<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>>.

technology innovation to our economic, political, and military success going forward—and the critical role of the private sector, including investors, innovators, entrepreneurs, and companies alike, in such innovation—it is critical that the United States act now to quickly and significantly shore up our ability to ensure we remains the technology capital of the globe, and that we and our allies, working together, are able to leverage joint technology innovation, research, and development, as well as combined production capabilities to gain a significant measure of economic independence from the PRC. Given our leading position today and the clear effort by China to try to take the pole position, if we fail to maintain this advantage now and into the future, we will have no one to blame but ourselves.

PREPARED STATEMENT OF LINDSAY GORMAN
SENIOR FELLOW FOR EMERGING TECHNOLOGIES, THE ALLIANCE FOR SECURING
DEMOCRACY AT THE GERMAN MARSHALL FUND OF THE UNITED STATES
JANUARY 18, 2024

Lindsay Gorman Testimony
 Page 2 of 13

Introduction

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

I lead a research and analysis team at the German Marshall Fund's Alliance for Securing Democracy, studying how democracies can together outcompete autocrats – chiefly the People's Republic of China (PRC) – in emerging technologies. I am also a Venture Scientist with Deep Science Ventures. I come at this question from the perspective of a technologist with academic training in quantum physics and artificial intelligence and first-hand experience researching the technologies we now recognize as critical to U.S. national competitiveness. I recently had the privilege of serving at the White House, where I crafted technology and national security competitiveness strategy across the U.S. government. I also developed initiatives to implement that strategy, including through the U.S.-EU Trade and Technology Council and Quad Critical and Emerging Technology Working Group. Both during my time at the German Marshall Fund and in government, I have had the opportunity and privilege of engaging extensively with officials, policy, and technology communities across the Atlantic on PRC technology matters from 5G and digital infrastructure to AI and international standards setting. Finally, I spent the first part of my career working with start-up companies and venture capital, including founding a firm looking at emerging technologies. The views I express in this testimony and before you are my own and should not be taken as representing those of my current or former employers.

Toward a New Mode of Techno-Economic Statecraft

The United States has spent decades investing in, inventing, and re-inventing new modes of warfare – from the Goldwater-Nichols Act to the first, second, and third offset strategies. And today, inspired in part by rapid capability-fielding in Ukraine, we are undergoing a transformation to enable the Pentagon to draw more effectively on private sector innovation for rapid capability deployment. Each of these offset strategies was aimed at a particular objective and a shift in adversary capability, largely in and around the role of nuclear weapons. Today, the United States's strongest autocratic rival is using tactics in economic, technological, and societal realms that a defense-first national security apparatus was not designed to counter. In the PRC, we face a competitor who wields its own economic power to coerce nations, businesses, and individuals to achieve its technology and national security objectives. This multi-sectoral competition has strained the post-Cold War view of international relations in which more economic engagement implied greater political – even democratic – proximity. The cost of doing business in China is often the hollowing out of technology advantages and IP, described as the greatest transfer of wealth in human history. The CCP also is clear-eyed about competition with the United States. According to Xi, “the United States is the biggest threat to China’s development and security.”¹

¹He, Bin (何斌), “Speech at Special Seminar for County-Level Leading Cadre to Study and Implement the 5th Plenum of 19th Central Committee” (在县级领导干部学习贯彻党的十九届五中全会专题研讨班上的发言), Qilian News (祁连新闻),

Lindsay Gorman Testimony
Page 3 of 13

So how does the United States best compete with an autocratic rival where that competition is playing out chiefly in non-traditional spheres of battle: technology, economy, and society, in addition to military capability build-ups? Much in the way the Cold War led to a society-wide reworking of our institutions towards great power competition, so too now do we need a rethink of our tools. A key element of this effort is building out a doctrine, toolkit, and alliances for techno-economic statecraft.

We are not starting from whole cloth. Some of these tools already exist, but many were designed for a different era, when the chief concern was preventing the development of Weapons of Mass Destruction (WMD).² The remit was far simpler: ensure that technology items with a ‘dual-use’ capability – i.e., those that could be used for both military and civilian applications – were used for the latter and not the former. Moreover, these dual applications often had clear signatures and relatively long timescales on which a civilian capability could transition to a WMD use. Nuclear energy vs. nuclear weapons is the canonical example, where uranium enriched above a certain threshold becomes weapons-grade and thus a proliferation concern.

These modes are outdated and unfit for our modern challenges for three reasons. First, straightforward distinctions and thresholds between military and civilian applications of emerging technologies in many cases do not exist. Emerging technologies like artificial intelligence, quantum information systems, advanced computing, and biotechnology are *inherently* dual-use. The same quantum computer that could revolutionize chemistry calculations and scientific discovery could break the encryption that secures our communications with submarines. The same synthetic biology and genomic engineering processes that could engineer novel cancer therapies could engineer pandemic pathogens. And the same computing capacity that fuels Large Language Models can fuel drone swarms or societal surveillance. AI is often described as falling into a class of technologies that economists refer to as ‘general-purpose technologies’ – akin to electricity, the steam engine, or the internal combustion engine.³ There are no thresholds to set when determining what constitutes a dual use of an internal combustion engine.

Second, the PRC has pursued an explicit strategy of military-civil fusion (MCF) that further blurs the lines of these domains and makes it difficult to have confidence that any civilian use will stay a civilian use. By sharing talent and resources, the PRC hopes that economic and military modernization can develop side-by-side and in ways that are mutually reinforcing. According to the Defense Department:

February 25, 2021, <http://www.qzianews.com/system/2021/02/25/013341147.shtml>; [2022-report-20th-party-congress.pdf](https://www.ucs.edu/sites/default/files/2022-02/2022-report-20th-party-congress.pdf) (ucsd.edu)

² *Advancing National Security and Foreign Policy Through Sanctions, Export Controls, and Other Economic Tools, Before the U.S. Senate Committee on Banking, Housing, and Urban Affairs*, 118th Cong. (2023) (statement by Kevin Wolf, Partner at Akin Gump Strauss Hauer & Feld LLP and Senior Fellow at the Center for Security and Emerging Technology)

³ Erik Brynjolfsson and Andrew McAfee, “The Business of Artificial Intelligence,” *Harvard Business Review*, July 18, 2017, <https://hbr.org/2017/07/the-business-of-artificial-intelligence>.

Lindsay Gorman Testimony
Page 4 of 13

The PRC's MCF development strategy encompasses six interrelated efforts: (1) fusing China's defense industrial base and its civilian technology and industrial base; (2) integrating and leveraging science and technology innovations across military and civilian sectors; (3) cultivating talent and blending military and civilian expertise and knowledge; (4) building military requirements into civilian infrastructure and leveraging civilian construction for military purposes; (5) leveraging civilian service and logistics capabilities for military purposes; and, (6) expanding and deepening China's national defense mobilization system to **include all relevant aspects of its society and economy for use in competition and war.**⁴ [emphasis added]

And third, not all the national security risks associated with PRC emerging technology acquisition and dominance fall into the military domain. Human rights abuses, the promotion of autocratic values and standards baked into emerging technologies, and strategic economic and technological dependence of critical supply chains fall outside the scope of structures aimed at the traditional conception of dual use.⁵

Today, a growing list of 'defensive technology measures' for techno-economic statecraft include:

- Export controls
- Sanctions
- Supply Chain Due Diligence
- Investment Screening
 - Inbound investment
 - Outbound investment
- Anti-dumping measures
- Research security
- Prosecution of IP theft
- Tariffs on high-tech industries

A new doctrine for techno-economic statecraft must survey and leverage U.S. and allied advantages (and realistically assess willingness to fuse these ecosystems), deepen capabilities, and define short-, medium-, and long-term objectives for technology competition. It must be supported by a robust analytical and intelligence apparatus and resourced appropriately. And it must blend proactive ('promote') tools with defensive ('protect') technology measures. On the

⁴ U.S. Department of Defense, "2022 Report on Military and Security Developments Involving the People's Republic of China 2022 Report on Military and Security Developments Involving the People's Republic of China", US Department of Defense, November 29, 2022.

⁵ Lindsay Gorman, "The U.S. Needs to Get in the Standards Game – With Like-Minded Democracies," Lawfare, April 2, 2020, <https://www.lawfaremedia.org/article/us-needs-get-standards-game%E2%80%944-minded-democracies>; Cyberspace Solarium Commission Report (United States Cyberspace Solarium Commission, 2020), <https://www.solarium.gov/report>; Paul Mozur and Don Clark, "China's Surveillance State Sucks Up Data. U.S. Tech is Key to Sorting It," New York Times, November 22, 2020, <https://www.nytimes.com/2020/11/22/technology/china-intel-nvidia-xinjiang.html>.

Lindsay Gorman Testimony
Page 5 of 13

latter, outpacing China no longer simply means outrunning the PRC but also impeding its capabilities in select game-changer and 'force-multiplier' technologies. The stated goal of National Security Advisor Jake Sullivan in the context of foundational semiconductors "to maintain as large of a lead as possible" will require the United States and its allies to **control capabilities, not only technologies**.

Emerging Technologies' Inputs: Considerations for Control

Critical to a strategy for techno-economic statecraft is the selection of objectives in critical technology areas that drive considerations for how their transfer may be controlled. I discuss several such considerations in the cases of AI, biotechnology, and quantum information technologies. All three can be thought of in terms of their data, software, and 'hardware' (or 'bio-ware') inputs. Hardware is the most straightforward to control, but new advances may render that focus insufficient.

Artificial Intelligence: Inputs to AI include data to train models on, algorithms to build those models and perform the training, and computing power to process this development.⁶ Pioneering controls on the PRC's AI capabilities issued on October 7, 2022 focused on hardware – exploiting a chokepoint to stifle the flow of ultra high-end semiconductor technology, specialized manufacturing tools, and manufacturing capacity to China. With complex controls including end user applications of the Entity List and Foreign Direct Product Rule, end use controls, PRC-wide controls, and restrictions on U.S. persons, they demonstrate a holistic approach to controlling capabilities. Netherlands and Japan enacted similar controls, though Germany, whose Zeiss and Trumpf laser and optoelectronics firms supply the Dutch ASML for lithography equipment, has not. Moreover, Chinese developers are already finding workarounds, and smuggling networks risk blunting the controls' effects. One glaring loophole is the ability to access equivalent processing power using cloud computing infrastructure. With the advent of frontier models, whether to restrict their application in specific end uses including military and human right abuses will need to be considered as well. Indeed, the most fraught elements of the Treasury Department's Advanced Notice of Proposed Rulemaking on outbound investment included the breadth of AI and the ability to circumvent military end-uses dependent on exclusive or primary use.⁷

Biotechnology: Inputs to biotechnology advances include: genetic material (DNA, RNA, genomes); data (such as genetic data); bioinformatics tools and advanced computing (such as software and algorithms for analyzing biological data); specialized biological components

⁶ Export Control Reform Implementation: Outside Perspectives, Hearing Before the U.S. Senate Committee on Banking, Housing, and Urban Affairs, 115th Cong. (2019) (statement of Ben Buchanan, Assistant Teaching Professor, School of Foreign Service, Senior Faculty Fellow, Center for Security and Emerging Technology, Georgetown University).

⁷ "Outbound Investment Program," U.S. Department of the Treasury, <https://home.treasury.gov/policy-issues/international/outbound-investment-program>; Department of the Treasury, "Provisions Pertaining to U.S. Investments in Certain National Security Technologies and Products in Countries of Concern," Federal Register Vol. 88 no. 155 (August 14, 2023); <https://www.govinfo.gov/content/pkg/FR-2023-08-14/pdf/2023-17164.pdf>.

Lindsay Gorman Testimony
Page 6 of 13

(molecules and materials harvested organically or synthetically produced); and specialized equipment (such as DNA sequencers or bioreactors). However, China's biomanufacturing ecosystem is highly developed, leading to strategic dependencies for the United States in advanced pharmaceutical ingredients and making prospects for technology controls difficult.⁸

The story of Beijing's genetic data rise is also one of failed defensive technology measures ill-adapted to a new reality. The PRC is amassing global bio data, taking advantage of partnerships with BGI, Huawei, and firms like WuXi App Tech, which has been associated with the popular genetics company 23andMe. Concerning pieces of China's biotechnology industry can be tied directly to U.S. partnerships. In 2012, Chinese biotech giant BGI received CFIUS clearance to acquire California-based Complete Genomics.⁹ Today, multiple BGI affiliates, including BGI Research and BGI Tech Solutions, have been placed on the U.S. Entity List for their collection and analysis of genetic data that risks contributing to PRC surveillance and monitoring, as well as the risk of diversion to military programs.¹⁰ However, BGI maintains a network of over 200 global subsidiaries, most of whom are not on the Entity List, allowing it access to genomic data from around the globe.¹¹ As innovators globally incorporate AI into biotechnology, these concerns will grow. Despite being flagged by CFIUS over a decade ago, the rise of BGI demonstrates a complete failure of imagination to envision the drivers of national power – a mistake the United States cannot afford to repeat and must attempt to better forecast.¹²

Quantum Computing and Information Technologies: In quantum information, the PRC has led in large-scale applications of quantum communications. These technologies aim to encrypt information using quantum key distribution (QKD) that may be theoretically more tamper-proof. In 2016, China launched the world's first quantum satellite (Micius) – enabled in part by German

⁸ Jeffrey Algray, et al., *Vision 2028: How China could impact the global biopharma industry* (McKinsey & Company, 2022), <https://www.mckinsey.com/~/media/mckinsey/industries/life%20sciences/our%20insights/vision%202028%20how%20china%20could%20impact%20the%20global%20biopharma%20industry/vision-2028-how-china-could-impact-the-global-biopharma-industry.pdf>

⁹ Securities and Exchange Commission, "BGI-Shenzhen and Complete Genomics, Inc. Receive CFIUS Clearance for BGI-Shenzhen's Proposed Acquisition of Complete Genomics, Inc. BGI-Shenzhen and Complete Genomics, Inc. Receive CFIUS Clearance for BGI-Shenzhen's Proposed Acquisition of Complete Genomics, Inc.," Securities and Exchange Commission, December 28, 2012,

¹⁰ *Countering China: Advancing U.S. National Security, Economic Security, and Foreign Policy*, Before the U.S. Senate Committee on Banking, Housing, and Urban Affairs, 118th Cong. (2023) (statement of Thea D. Rosman Kendler, Assistant Secretary of Commerce for Export Administration).

¹¹ Advancing Growth, Knowledge, and Innovation through Higher Education, Before the U.S.-China Economic and Security Review Commission hearing on

"China's Challenges and Capabilities in Educating and Training the Next Generation Workforce," 118th Cong. (2023) (statement of Anna B. Puglisi, Director of Biotechnology Programs at Center for Security and Emerging Technology, Georgetown University).

¹² *Commanding Heights: Ensuring U.S. Leadership in Critical and Emerging Technologies*, Before the House Select Committee on the Competition Between the United States and the Chinese Communist Party, 118th Cong. (2023) (statement of Lindsay Gorman, Senior Fellow and Head of the Technology and Geopolitics Team, Alliance for Securing Democracy, The German Marshall Fund of the United States).

Lindsay Gorman Testimony
Page 7 of 13

and EU funding.¹³ It continues to test technologies through its Quantum Experimentation at Space Scale (QUESS) quantum-enabled communications satellite, including sending quantum keys for use in quantum cryptography between Austrian and Chinese ground stations. Quantum communications is also an increasing area of Sino-Russian collaboration, as the no-limits partnership blossoms in the technology and information arena. In December 2023, Chinese and Russian scientists demonstrated the encrypted communication using quantum key distribution of images between ground stations in Urumqi, Xinjiang and outside Moscow, by way of China's quantum satellite.¹⁴

However, the real competition in quantum computing is the race to a universal fault-tolerant quantum computer, which carries the ability to break the classical encryption services that modern secure systems from our intelligence apparatus to our nuclear deterrent rely on. There is a case, therefore, to be made for taking steps to put the United States in a significant leadership position towards this goal. Concerns over military applications in counter-stealth and counter-submarine technologies as well as the potential to break classical encryption drove Entity List additions of PRC quantum technology entities including QuantumCTek. And some post-quantum cryptography algorithms are subject to BIS export licenses. Proposed outbound investment controls would prohibit covered investments into quantum computers and components (such as cooling systems), quantum sensors, quantum networking and communication systems, as well as low-temperature semiconductors operating under 4.5 Kelvin used for quantum chips.¹⁵ Here, technology forecasting and tracking will be essential to defensive measures, as preferred approaches are still evolving with scientific research.¹⁶

Building and Resourcing the Defensive Technology Measures Toolkit

Just as we have spent decades resourcing the U.S. military for strategic advantage, so too we must resource the tools of techno-economic statecraft. At the heart of this effort is the Commerce Department and specifically its Bureau of Industry and Security, charged with implementing and enforcing export controls on critical and emerging technologies and helping to secure the nation's supply chains.

Here, I offer three categories of recommendations:

¹³ Sandra Petersmann and Esther Felden, "China's quantum leap – Made in Germany," *Deutsche Welle*, June 16, 2023, <https://www.dw.com/en/chinas-quantum-leap-made-in-germany/a-65890662>.

¹⁴ Xu Ning, "How important is it for China and Russia to cooperate in testing quantum satellite communications? Who is stronger in the United States and China?" *VOA News*, January 11, 2024, <https://www.voachinese.com/a/us-china-russia-quantum-communication-20240110/7434011.html>.

¹⁵ "Outbound Investment Program," U.S. Department of the Treasury, <https://home.treasury.gov/policy-issues/international/outbound-investment-program>; ANPRM Department of the Treasury, "Provisions Pertaining to U.S. Investments in Certain National Security Technologies and Products in Countries of Concern," Federal Register Vol. 8 no. 155 (August 14, 2023): <https://www.govinfo.gov/content/pkg/FR-2023-08-14/pdf/2023-17164.pdf>.

¹⁶ Edward Parker, *Promoting Strong International Collaboration in Quantum Technology Research and Development* (RAND Corporation, 2023), <https://www.rand.org/pubs/perspectives/PEA1874-1.html>; Edward Parker, et al., *An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology* (RAND Corporation, 2022), https://www.rand.org/pubs/research_reports/RRA869-1.html.

1. **Significantly expand U.S. and allied analytical capacity.** In order to make informed decisions on which levers of the techno-economic toolkit to pull, the United States needs a significant analytical capability that can forecast technology areas and needs, analyze the effects of techno-economic measures, assess U.S. leadership potential and China's indigenization prospects in critical technology areas, and wargame techno-economic actions and responses. As Daleep Singh told this Committee, economic wargames should model the extensive wargaming the Pentagon conducts for military affairs.¹⁷

Establish a National Technology Competitiveness Analysis Center (NTCAC) modelled after National Counterterrorism Center or National Counterintelligence Center to conduct red-blue team analyses on critical and emerging technology ecosystems. This center should draw on expertise across the federal government – such as in the national labs and DOD – in addition to industry analysis. It should also include input from the intelligence community on areas of PRC IP theft, the state of technology transfer, and identification and tracking of chokepoints. This center could be housed at the Commerce Department and report to the Secretary's Office with a dotted line reporting structure to the ODNI. It should include a wargaming cell dedicated to conducting red-blue team exercises in the techno-economic sphere.

2. **Increase funding for personnel, but also technology tools.** BIS's overall budget has not kept pace with its growing responsibilities. In the Commerce Department's FY 2023 budget request, BIS identified more than \$53 million in unfunded requirements.¹⁸ These included ICTS supply chain security, additional Special Agents and Enforcement analysts to keep pace with the rise cases related to China and Russia, industry survey studies, the use of data to assess the effectiveness of licensing systems, and expanding a partnership with Canada on securing supply chains.¹⁹ In FY2024, that number was \$14 million, including elements of developing a modern Data Science and Impact Analysis Capability.²⁰ The FY 2024 budget requests a \$31 million increase in BIS budget from FY 2023.

Congress should at minimum fully fund this request, \$16.866 million of which accounts for inflationary adjustments, and increase BIS's FY 2024 budget to fund its \$14 million in unfunded priorities.

¹⁷ *Advancing National Security and Foreign Policy Through Sanctions, Export Controls, and Other Economic Tools, Before the U.S. Senate Committee on Banking, Housing, and Urban Affairs, 118th Cong. (2023)* (statement by Daleep Singh, former Deputy National Security Advisor for International Economic and Deputy Director of the National Economic Council).

¹⁸ Gregory C. Allen, Emily Benson, and William Alan Reinsch, *Improved Export Controls Enforcement Technology Needed for U.S. National Security* (Center for Strategic and International Studies, 2022), <https://www.csis.org/analysis/improved-export-controls-enforcement-technology-needed-us-national-security>.

¹⁹ U.S. Department of Commerce, Bureau of Industry and Security, *Fiscal Year 2023 President's Budget Request, 2023*, <https://www.commerce.gov/sites/default/files/2022-03/FY2023-BIS-Congressional-Budget-Submission.pdf>.

²⁰ U.S. Department of Commerce, Bureau of Industry and Security, *Fiscal Year 2024 President's Budget Request, 2024*, <https://www.commerce.gov/sites/default/files/2023-03/BIS-FY2024-Congressional-Budget-Submission.pdf>.

Lindsay Gorman Testimony
Page 9 of 13

Moreover, U.S. techno-economic competition should be resourced with cutting-edge tools, including leveraging technologies like AI and data science to track smuggling networks that help evade controls, and keep pace with the proliferation of subsidiaries and shell companies that regularly spin up from companies on the Entity List. Automatic systems could flag new entities that may be owned in whole or in part by listed entities. Knowledge graphs or link-analysis tools could modernize BIS's ability to trace smuggling networks, track shell companies, and fuse data from Chinese-language technology and financial sources to discern whether and how controls were being violated. The U.S. Army, for example, uses such software to manage a 3 TB database to forecast logistical needs for replacement parts, calculate mean time for failure rates, perform multi-dimensional cost comparisons, and inform budget requirements – slashing needed employee hours by 88%.²¹ MITRE's Cygraph analyzes large loads of isolated data and optimizes pattern recognition to find and stop cyber-attacks.²² Tools like expanded versions of the Australian Strategic Policy Institute's China Defence Universities Tracker can help analysts discover and prevent export controls evasion by elucidating the complex linkages among PRC actors with military-industrial ties. The datasets relevant to export enforcement are likely harder to come by, but no less critical. Finally, controlled hardware parts could embed geolocation tagging so that export enforcement analysts could track their movement globally.²³

To address concerns around data security and influence stemming from autocratic ICTS platforms, Congress should:

- a. Pass legislation on a risk-based framework for assessing ICTS platforms operating in the United States and lead by example on autocratic apps. Develop an international coalition a comprehensive, risk-based framework for autocratic internet apps – democratic allies and partners to develop a comprehensive framework for addressing the threats posed by authoritarian internet apps and critical information infrastructure. TikTok and Huawei are not one-offs. We cannot treat them as such. As we head into the 2024 election season with more Americans than ever getting their news from a platform whose parent company answers to the CCP, there is true urgency.
- b. Pass Federal Data Privacy and Data Security Legislation. We cannot solve technology espionage through data privacy alone, but we can close loopholes and punish excess abuses.

²¹ Neo4j, "Neo4j Keeps the Army Running by Tracking Equipment Maintenance," accessed January 17, 2024, <https://neo4j.com/case-studies/us-army/>.

²² Neo4j, "Graph Technology Powers Cybersecurity Situational Awareness That's More Scalable, Flexible & Comprehensive," accessed January 17, 2024, <https://neo4j.com/case-studies/mitre/>.

²³ Chris Miller and Jordan Schneider, "How to Stop Our High-Tech Equipment From Arming Russia and China," *New York Times*, December 29, 2023, <https://www.nytimes.com/2023/12/29/opinion/chips-semiconductor-china-russia-military.html>.

3. **Build capacity among U.S. allies and partners on novel techno-economic statecraft tools and approaches.** As business groups from the Semiconductor Industry Association to the National Foreign Trade Council have exhorted, unilateral controls harm U.S. businesses relative to allied foreign competitors, as these competitors simply backfill the void created by U.S. exits in the context of remaining market demand.²⁴ The extent and timescale over which this backfilling is possible depends on the degree to which U.S. industry corners the market, but unilateral controls do risk the United States shooting itself in the foot, especially if such controls end up being insufficient to meaningfully limit PRC capabilities at issue due to allied backfilling. For these reasons, multilateral action is a necessity. The challenge is that democratic nations are experimenting with new tools, new authorities, new uses, and new modes of statecraft themselves, at the same time as there is a need to implement these measures jointly.

On export controls and outbound investment screening, FIRRMA's expansion of CFIUS for inbound investment screening provides a strong model for international cooperation. FIRRMA included three provisions to aid U.S. allies and partners in strengthening their own investment screening mechanisms²⁵:

- ***A formal process for information transfer*** to allow for shared understanding of national security rationales for investment screening among U.S. allies and partners.
- ***Outreach and technical support.*** Treasury conducted international outreach and offered technical support and capacity-building for countries interested in constructing investment review mechanisms.
- ***Incentives to strengthen screening mechanisms.*** At the same time, FIRRMA's implementing regulations created a category of "excepted foreign states, whose covered investments into the United States could be subject to less rigorous review, provided these states had developed robust enough investment screening mechanisms in their own right."

While incomplete, this process has been a resounding success. In 2019, the European Commission announced guidelines to encourage member states to stand-up formal investment review procedures. As of October 2023, 21 EU member states had screening mechanisms (up from 11 in 2017), and several others are in the process of adopting an investment review regime.

²⁴ Semiconductor Industry Association, "Comments of the Semiconductor Industry Association on Advanced Notice of Proposed Rulemaking regarding Review of Controls for Certain Emerging Technologies" (public comment, 2019), <https://www.regulations.gov/document/BIS-2018-0024-0130>; National Foreign Trade Council, "Comment on Advanced Notice of Proposed Rulemaking Regarding Review of Controls for Certain Emerging Technologies" (public comment, 2019), <https://www.regulations.gov/document/BIS-2018-0024-0081>.

²⁵ John S. McCain National Defense Authorization Act for Fiscal Year 2019, H.R. 5515, 115th Cong. (2018).

Lindsay Gorman Testimony
Page 11 of 13

This international technical assistance capacity should be expanded in the context of outbound investment screening and replicated at the Commerce Department in the context of export controls.²⁶

Complementary to this effort, the United States should:

- a. Build out joint competitive analytic capacity with key allies and partners. The Quad Critical and Emerging Technology effort on Horizon Scanning is a first step, but this effort needs deeper resourcing, a more permanent commitment, and the eventual involvement of Five Eyes partners. The US-EU Trade and Technology Council's work on investment security can be a natural jumping off point for this cooperation in the transatlantic context, where the United States should seek to build capacity and shared understanding at the European Commission, even as many measures will be implemented at the Member State level.
- b. Invest in the U.S.-EU Trade and Technology Council and Quad for semi-permanence. Congress should build a line-item into the State and Foreign Operations budget to support the TTC over a five-to-10-year timescale. Connective tissue is important, and bureaucratic mechanisms take time and effort to stand up and to build trust. Congress can help insulate this mechanism from changing political winds in the United States, while providing the means for its strategic evolution and adaptation over time.
- c. Guided de-risking: Adopt a framework with key allies and partners to measure the PRC's technological control in a given country or region. My team at GMF has developed a proof of concept of this analysis on China's Digital Technology Stack.²⁷ Building a true allied understanding of China's penetration in global technology ecosystems is the first step towards robust allied competitiveness and a common operating picture of the threat. Such analysis can also guide G7 and multilateral development efforts.
- d. Coordinate targeted outbound investment screening with allies and partners, including information sharing mechanisms. While discussions on outbound investment screening are further ahead in the U.S., aligning approaches and critical technology sectors with Europe can help drive allied competitiveness. At a minimum, screening tools should include restrictions on private investment to entities on the Entity List and Treasury's NS-CMIC. The U.S. must ensure

²⁶ European Commission, "EU foreign investment screening and export controls help underpin European security," October 19, 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5125.

²⁷ Lindsay Gorman, *A Future Internet for Democracies: Contesting China's Push for Dominance in 5G, 6G, and the Internet of Everything* (The Alliance for Securing Democracy, 2020), <https://securingdemocracy.gmfus.org/future-internet/>; Bryce Barros, Nathan Kohlenberg, and Etienne Soula, *China and the Digital Information Stack in the Global South* (The Alliance for Securing Democracy, 2022), <https://securingdemocracy.gmfus.org/china-digital-stack/>.

Lindsay Gorman Testimony
Page 12 of 13

coordination amongst these lists and use sector-specific outbound investment screening to close loopholes in export controls aimed at exploiting chokepoints.

- e. Develop a new multilateral export control regime for critical and emerging technologies that includes a strong consideration of human rights abuses. Existing Cold War-era regimes such as the Wassenaar Arrangement are inadequate to address the explosion of dual-use technology across all segments of society as well as their democracy and human rights implications. Many allied export control regimes lack or are just developing the capacity to implement end-user controls. Few are structured to account for human rights abuses, yet multilateralizing U.S. defensive policies is essential to their success.

U.S. allies and partners have an extremely strong hand to play if they act thoughtfully, decisively, and multilaterally in building out the doctrine and tools of techno-economic statecraft. I look forward to your questions.

**RESPONSES TO WRITTEN QUESTIONS OF CHAIR BROWN
FROM EMILY KILCREASE**

Q.1. Establishing U.S. supply chains for solar and other technologies is essential for American energy security. For instance, Chinese-headquartered companies now make up 99 percent of the world's solar wafer and 80 percent of the world's polysilicon production—two core components that make up half the value of the solar panel.

What recommendations do you have to make sure the U.S. is taking a whole-of-Government approach to securing clean energy supply chains, like solar? How can and should the U.S. Government support domestic manufacturing growth to meet our energy security and clean energy goals?

A.1. As¹ the U.S. Government takes action to address climate change, it must do so in a way that strengthens U.S. energy security and the resiliency of U.S. energy supply chains. The urgent need to address climate change must be balanced with the risk of creating a new dependency on China, which is the dominant global producer of clean energy technologies. An effective U.S. clean energy strategy will spur U.S. clean energy innovation and manufacturing, while addressing the economic, national security, and human rights concerns associated with imports of Chinese clean energy products. The United States should:

Invest in innovation and capacity throughout the clean energy technology life cycle: The United States has historically had a good track record in funding early-stage research and development in clean energy technologies, as well as using regulatory or other incentives to increase demand for clean energy products.² The United States has been less successful in strengthening domestic manufacturing capacity, leading to a perverse consequence in which U.S. demand for clean energy technologies (including demand that is supported by U.S. Government policies) can create a surge in imports, notably from China.³ The Inflation Reduction Act (IRA) provides an effective response to this challenge, by creating a sustainable foundation for cost-competitive manufacturing of critical clean energy technologies domestically. The U.S. Government should support strong implementation of the IRA's clean energy provisions, while also investing in the skilled workforce needed to build a durable clean energy manufacturing base in the United States.

¹ These responses reflect the personal views of the author alone. As a research and policy institution committed to the highest standards of organizational, intellectual, and personal integrity, the Center for a New American Security (CNAS) maintains strict intellectual independence and sole editorial direction and control over its ideas, projects, publications, events, and other research activities. CNAS does not take institutional positions on policy issues and the content of CNAS publications reflects the views of their authors alone. In keeping with its mission and values, CNAS does not engage in lobbying activity and complies fully with all applicable Federal, State, and local laws. CNAS will not engage in any representational activities or advocacy on behalf of any entities or interests and, to the extent that the Center accepts funding from non-U.S. sources, its activities will be limited to bona fide scholastic, academic, and research-related activities, consistent with applicable Federal law. The Center publicly acknowledges on its website annually all donors who contribute.

² Jonas Nahm, "Reimagine: Clean Energy Technology and U.S. Industrial Policy" (Washington, DC: Center for a New American Security, September 7, 2022), <https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS-Report-Reimagine-Clean-Energy-Tech-final-v2.pdf>.

³ Nahm, "Reimagine: Clean Energy Technology and U.S. Industrial Policy".

Establish innovative financing mechanisms: In addition to the incentives provided by the IRA, the U.S. Government should create additional innovative financing mechanisms to support clean energy production domestically, such as the Industrial Finance Corporation of the United States (IFCUS). The IFCUS, or similar entity, would be a Government-owned corporation, governed by an independent board, that would provide debt and equity financing to U.S. clean energy companies to support domestic manufacturing. Such an entity could focus on technologies that are critical to future U.S. energy security but that private markets are not incentivized to support. In contrast to the IRA, which is built on tax incentives, an IFCUS mechanism could ultimately return money to the U.S. Treasury as its investments generate a return.⁴

Build alternative sources of critical minerals supply with close partners: Critical minerals are essential to clean energy supply chains, and the United States does not currently have reliable, diversified supply of these minerals. According to the U.S. Department of Energy, over 80 percent of U.S. critical minerals supply comes from foreign sources.⁵ Where possible, the United States should invest in the responsible extraction and processing of critical minerals domestically, including through the use of Defense Production Act authorities.⁶ However, recognizing that domestic supply is unlikely to fully meet domestic needs, the United States must also work with international partners to bolster supply that can meet their collective needs. Congress should support initiatives such as the Minerals Security Partnership, in which the United States works with close partners (Australia, Canada, Finland, France, Germany, Japan, the Republic of Korea, Sweden, the United Kingdom, and the European Union) to coordinate efforts to strengthen critical mineral supply chains.⁷

Adopt a risk-based approach to deployment of Chinese clean energy technologies in the United States: Given China's dominant role in global clean energy supply chains, the United States cannot entirely avoid the use of Chinese technologies if it wants to make progress on climate objectives. At the same time, not all deployments of Chinese technologies present similar risks. U.S. policies should restrict the deployment of Chinese technologies in applications that would involve direct interconnection with the U.S. grid or otherwise present unacceptable risks to the cybersecurity of U.S. critical infrastructure. In less sensitive applications, the United States must maintain a diverse source of supply, either through increased domestic production or through friendshoring policies, to avoid creating a dependency on China that would present energy security and national security risks.

⁴Emily Kilcrease and Emily Jin, "Rebuild: Toolkit for a New American Industrial Policy", (Washington, DC: Center for a New American Security, September 2022), <https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/Rebuild-OCEA-2022-Final.pdf>; Nahm, "Reimagine: Clean Energy Technology and U.S. Industrial Policy".

⁵"Developing a Domestic Supply of Critical Minerals and Materials", U.S. Department of Energy, Office of Fossil Energy and Carbon Management, February 6, 2024, <https://www.energy.gov/fecm/articles/developing-domestic-supply-critical-minerals-and-materials#>.

⁶Joshua Busby, Emily Holland, Morgan Bazilian, and Paul Orszag, "The Defense Production Act's Role in the Clean Energy Transition", *Lawfare*, July 17, 2023, <https://www.lawfaremedia.org/article/the-defense-production-act-s-role-in-the-clean-energy>.

⁷"Minerals Security Partnership", U.S. Department of State, accessed March 11, 2024, <https://www.state.gov/minerals-security-partnership/>.

**RESPONSES TO WRITTEN QUESTIONS OF
SENATOR CORTEZ MASTO FROM EMILY KILCREASE**

Q.1. In your opinion, how effective are the current dual-use export controls and foreign investment screening mechanisms in addressing the possibility of U.S. innovation enhancing PLA capabilities?

A.1. The U.S. system for screening foreign investment in the United States, as implemented by the Committee on Foreign Investment in the United States (CFIUS), is largely effective in mitigating the risk that U.S. innovation, transferred via an investment, can enhance PLA capabilities. As one indicator, Chinese foreign direct investment (FDI) in the United States has plummeted in recent years, and unlike FDI from other countries, has not rebounded from pandemic-era lows.¹ CFIUS must remain vigilant to ensure the efficacy of its work, and certain updates (noted in the answer to the next question) can support its efforts to remain ahead of evolving threat environments.

The U.S. Government is using dual-use export controls to address an increasing array of national security and foreign policy concerns. While dual-use export controls were previously a more limited mechanism to prevent destabilizing accumulations of conventional weapons, they are now being used as a leading tool to manage the strategic competition with China, degrade Russian military capabilities, and address human rights abuses, among other issues. While export controls can be used effectively in this broader context, doing so requires a significant investment in Government capacity.

The budget for the Bureau of Industry and Security (BIS), the lead agency for administering dual-use export controls, has remained flat in real terms for over a decade. Congress should increase funding, with a focus on building analytic capabilities within BIS, establishing an office charged with evaluating the effectiveness of dual-use export controls, strengthening international outreach, and bolstering enforcement. Additional details are provided in my written testimony.²

It is worth emphasizing the importance of international coordination in enhancing the effectiveness of U.S. dual-use export controls. The effectiveness of unilateral controls erodes over time, as firms from other countries backfill U.S. technology. Most worrisome, over time U.S. technology may be designed out of international supply chains, harming long-term U.S. technology competitiveness.³ In addition to considering new multilateral regimes (as noted in the answer to a separate question from Senator Van Hollen), the United States must have robust international outreach functions to coordinate policies with key partners and provide technical assistance and intelligence support. While U.S. efforts to coordinate with

¹Bureau of Economic Analysis International Economic Accounts Factsheets, (International Trade and Investment Country Facts—China; accessed September 10, 2023), <https://apps.bea.gov/international/factsheet/factsheet.html#650>.

²“U.S. Economic Security Strategy, Authorities, and Bureaucratic Capacity”: Hearing Before the U.S. Senate Committee on Banking, Housing, and Urban Affairs, 118th Cong. (2024) (statement of Emily Kilcrease, Senior Fellow and Director, Energy, Economics, and Security Program, CNAS), <https://www.banking.senate.gov/imo/media/doc/kilcrease-testimony-1-18-24.pdf>.

³Sarah Bauerle Danzman and Emily Kilcrease, “The Illusion of Controls: Unilateral Attempts To Contain China’s Technology Ambitions Will Fail”, *Foreign Affairs*, December 30, 2022, <https://www.foreignaffairs.com/united-states/illusion-controls>.

Dutch and Japanese counterparts on recent controls on semiconductor manufacturing equipment is encouraging, much more regular and far-reaching coordination is needed.

Finally, dual-use export controls can be made more effective by establishing a set of complementary controls on outbound U.S. investment in China. Certain U.S. investments may advance indigenous Chinese capabilities in sensitive technologies and erode the effectiveness of export controls. Congress can act to address this risk by passing legislation to establish a targeted set of outbound investment controls designed to work in tandem with dual-use export controls to protect U.S. innovation and technology leadership in national security technologies.⁴

Q.2. Given your role in drafting CFIUS reform regulations, can you elaborate on any specific improvements or gaps in the current foreign investment screening process, especially concerning critical technology and sensitive personal data?

A.2. CFIUS would benefit from an expanded definition of “critical technology.” Currently, critical technology is defined by reference to export control authorities and CFIUS does not have the authority to define its own lists of critical technology. This approach generally makes sense, as it promotes coherence between the two sets of authorities and leverages the technical expertise resident in the export control agencies. However, in certain instances, CFIUS has a national security interest in reviewing foreign investments in U.S. businesses that do not make export-controlled technology. One example is in the artificial intelligence (AI) space, where the level of export controls is relatively low but the potential for national security risk, particularly associated with frontier AI systems, is growing exponentially. Congress should consider providing CFIUS with a limited new authority to define a set of “technologies controlled for investment purposes” that would be an additional category within the definition of “critical technologies” to address these concerns. Additional technical detail is provided in my written testimony.⁵

The single most important thing that Congress can do to improve CFIUS’s work related to sensitive personal data is pass comprehensive data security and data privacy legislation. CFIUS has a well-established practice of addressing national security risks associated with sensitive personal data, as these risks arise in the context of a foreign investment. Too often, CFIUS must take action to address these risks simply because it is the only authority able to do so. This is a drain on CFIUS bandwidth and leads to a patchwork approach to data security and data privacy. The administration’s recent Executive order on data security is an important first step in

⁴“Principles and Policy Options for Designing Better Investment Barriers”: Hearing Before the U.S. House of Representatives Subcommittee on National Security, Illicit Finance, and International Financial Institutions of the Committee on Financial Services, 118th Cong. (2024), (statement of Emily Kilcrease, Senior Fellow and Director, Energy, Economics, and Security Program, CNAS), <https://docs.house.gov/meetings/BA/BA10/20240130/116767/HHRG-118-BA10-Wstate-KilcreaseE-20240130.pdf>.

⁵Kilcrease, “U.S. Economic Security Strategy, Authorities, and Bureaucratic Capacity”.

remedying this, but Congress must act to address the broader systemic issues related to data security and data privacy.⁶

**RESPONSES TO WRITTEN QUESTIONS OF
SENATOR VAN HOLLEN FROM EMILY KILCREASE**

Q.1. Ms. Gorman and Ms. Kilcrease, you both testified to the importance of collaboration to help strengthen our competition strategy, calling for better coordination among Federal agencies and for improved multilateral cooperation with our partners and allies.

In what specific ways should we better organize and leverage the tools at our disposal to promote multilateral cooperation to more effectively advance our competition strategy?

A.1. U.S. competition strategy must involve both defensive and proactive components. On the defensive elements, the United States should deepen cooperation with key partners on economic security policy tools, such as export controls, inbound investment screening, outbound investment controls, and data security. The guiding principle should be that the United States and its partners treat similar commercial transactions involving similar national security risks in a similar manner. This will strengthen the collective posture of U.S. and partner countries relative to strategic competitors, while also avoiding the negative impacts on U.S. competitiveness that can arise if U.S. partners have more permissive policies.

Ultimately, the United States should strive towards a multilateral regime that aligns U.S. policy on economic security tools with that of its partners. Such a mechanism would primarily serve as an information-sharing and coordination mechanism, with countries responsible for implementing agreements in their domestic processes. The objectives of the new regime would be to:

- “Promote international security and common security of the member Nations;
- Prevent the destabilizing accumulations of conventional or emerging weapons globally and prevent the transfer of dual-use technologies for such weapons to countries of concern;
- Promote the technological leadership in science, technology, engineering, and manufacturing sectors, including in foundational and emerging technology areas, that are material to national security and foreign policy of the member States; and
- Support the protection of human rights and democratic institutions.”¹

In support of these broader objectives, participating countries could seek to advance a shared assessment of the threat presented by China and other strategic competitors, identify technologies that are important to the national security of the participating members

⁶ Exec. Order No. 14,117, 89 FR 15421, (February 28, 2024), <https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related>.

¹ “Challenging China’s Trade Practices: Promoting Interests of U.S. Workers, Farmers, Producers, and Innovators”: Hearing Before the U.S.-China Economic and Security Review Commission, 117th Cong. (2022), (statement of Emily Kilcrease, Senior Fellow and Director, Energy, Economics, and Security Program, CNAS), <https://s3.us-east-1.amazonaws.com/files.cnas.org/backgrounds/documents/CNAS-Emily-Kilcrease-USCC-Testimony-04.14.2022-Hearing.pdf>.

and that should be subject to joint controls (including in the export control or investment control context), and align institutional processes and policies in each country. It is unlikely that the United States or other countries would agree to binding rules on issues related to national security, but the coordination, information-sharing, and norm-setting functions of a regime as outlined here would substantially enhance alignment between the United States and key partners on economic security issues.

U.S. competition policy cannot be only defensive, however. The United States must proactively seek to advance U.S. competitiveness in global markets. As the United States proceeds with a necessary derisking of economic ties with China, it must compensate for lost economic opportunity by building markets elsewhere. It must do so in a manner that reflects new priorities for U.S. trade policy, such as supply chain resiliency, economic security, and labor and environment protections. The United States should pursue economic security agreements to enhance resiliency and integration with key partners in critical sectors.² Such agreements could focus on aligning economic security and industrial policies, enhancing competition and innovation in critical technology areas, and strengthening labor, environment, and digital trade standards in trading partner countries.

Q.2. While it is preferable to secure multilateral cooperation through voluntary participation, under what circumstances should the United States use secondary sanctions to achieve our goals?

A.2. Secondary sanctions are a powerful tool, as they extend the reach of U.S. sanctions extraterritorially and cover even those transactions that do not involve a U.S. person.³ They can be an important enforcement tool to address sanctions evasion or transshipment through third party countries. For example, the threat of secondary sanctions appears anecdotally to have had a chilling effect on banks in third party countries (e.g., Turkey) that may have been financing shipments of critical goods to Russia.⁴ While secondary sanctions are largely a U.S. tool, the authorization of these secondary sanctions appears to have been well coordinated with the coalition of countries imposing sanctions on Russia, enhancing the legitimacy and effectiveness of the sanctions effort.

The United States should exercise caution when considering secondary sanctions on close allies. The threat of secondary sanctions was politically damaging to the U.S.-European relationship, for example, after the United States pulled out of the Iran nuclear deal and sought to prevent European companies from engaging with Iranian counterparts.⁵ Fears of such action were part of the motivation for Europe to develop a blocking statute to protect their companies from exposure to U.S. sanctions. In future sanctions sce-

²Emily Kilcrease, “No Winners in This Game: Assessing the U.S. Playbook for Sanctioning China” (Washington, DC: Center for a New American Security, December 1, 2023), 66, <https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/EES-No-Winners-Final-1.pdf>.

³Jason Bartlett and Megan Ophel, “Sanctions by the Numbers: U.S. Secondary Sanctions” (Washington, DC: Center for a New American Security, August 26, 2021), <https://www.cnas.org/publications/reports/sanctions-by-the-numbers-u-s-secondary-sanctions>.

⁴Beril Akman, Asli Kandemir, and Firat Kozok, “Turkish Banks Tighten Screws on Russia Over Fear of U.S. Sanctions”, *Bloomberg*, January 17, 2024, <https://www.bloomberg.com/news/articles/2024-01-17/turkish-banks-tighten-screws-on-russia-over-fear-of-us-sanctions>.

⁵Bartlett and Ophel, “Sanctions by the Numbers: U.S. Secondary Sanctions”.

narios involving China, secondary sanctions could lead to a divisive wedge between the United States and allies at a moment when signaling unity is a political imperative. It would also put the United States in an uncomfortable enforcement position, as it would need to be willing to enforce the secondary sanctions by punishing companies from allied countries.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR WARNOCK FROM EMILY KILCREASE

Q.1. You have noted that the United States has been relatively restrained in levying sanctions on the People's Republic of China, specifically stating, "To date, the United States has exercised restraint in using financial sanctions against Chinese targets, with notable exceptions related to human rights or support for Iran."¹ You also point out that "sanctioning China represents a challenge more complex than any other in the modern era of sanctions."²

As China continues to posture itself on the side of America's adversaries, like Iran and Russia, how can we best ensure that our sanctions have the intended effect and deter bad behavior?

A.1. An effective sanctions posture vis-a-vis China will require a nuanced mix of strategic restraint paired with deliberate efforts to build credibility of the U.S. sanctions threat. The United States has few good options when it comes to sanctioning China, given the intermingled nature of U.S. and Chinese supply chains and the role that China plays as a major trading partner with most of the globe. The one area of clear sanctions power is in the financial sector, where the United States can leverage the essential role of the U.S. dollar in global finance to place broad pressure across the Chinese economy and to target specific entities. The United States should preserve this leverage for times of genuine crisis or conflict, as premature efforts to weaponize the U.S. dollar would erode the potency of U.S. financial sanctions.³

At the same time, the United States must clearly signal its ability and willingness to escalate sanctions, including in the financial sector, should China cross certain geopolitical redlines. Ideally, such signaling would occur in partnership with the G7 or other close U.S. partners to demonstrate a united resolve to use sanctions tools to deter or respond to PRC actions that are against U.S. interests. U.S. credibility today is uncertain, as the PRC could assess that the United States is unwilling to accept the costs of harsh sanctions or that it would be unable to secure support from other international partners. These dynamics dangerously undercut the deterrent effect that sanctions can have.

One way to enhance the credibility of the sanctions threat is to strengthen the strategic planning process for the use of sanctions and other economic tools. While such planning is routine in the military community, sanctions policy is too often developed in an

¹Emily Kilcrease, "No Winners in This Game, Center for New American Security" (Dec. 2023), <https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/EES-No-Winners-Final-1.pdf> at 33.

²Id.

³Emily Kilcrease and John Hughes, "It's Not Time To Hit China With Financial Sanctions—Yet", *The Hill*, January 16, 2024, <https://thehill.com/opinion/international/4411407-its-not-time-to-hit-china-with-financial-sanctions-yet/>.

ad hoc or reactive manner. The economic agencies, with support from Congress, should institutionalize a sanctions strategic planning process, which can prepare for a range of potential future crisis or conflict scenarios and game out the geopolitical impact and economic consequences of using different sanctions strategies. This work should be done with an eye to integrating planning efforts with the military community and with international partners. The Government must also be constantly assessing the effectiveness of its sanctions tools, particularly as new and innovative tools continue to be rolled out (e.g., oil price cap, foreign direct product rules). While Treasury has an office tasked with assessing the impact of financial sanctions, Commerce does not have a comparable office for export controls, which are increasingly being used to deal with a range of foreign policy and national security problems.

Sanctions credibility also requires strong enforcement of those sanctions already in place. The Government has an acute need for expanded enforcement resources. As is clear in the Russia context, sanctioned States show a remarkable ability to adapt and develop sanctions evasion schemes, requiring sustained U.S. enforcement actions to maintain the pressure of sanctions throughout a protracted conflict.

Ultimately, the most effective sanctions posture will be one that recognizes the clear limits of U.S. sanctions and considers sanctions as just one tool that, in tandem with other instruments of national power, can be used to advance U.S. foreign policy interests. The limits of sanctions heighten the need for a more integrated planning process that appropriately places sanctions alongside all instruments of national power in building integrated deterrence strategies for China.

Q.2. How can we better target sanctions to maximize their impact on decision makers, while minimizing their impact on poor communities who have little say over the activities of those in power?

A.2. “Smart sanctions” are intended to target specific actors within a political system, rather than placing broad, damaging pressure across an entire economy. The smart sanctions approach was developed in recognition of the negative effects that sanctions can have throughout a country, including on those communities with no connection to political elites. In theory, a smart sanctions approach would target sanctions to those individuals, Government entities, or organizations directly involved in the problematic behavior. In certain sanctions contexts, this approach can mitigate unintended consequences for the broader population.

In practice, however, impacts are difficult to contain once sanctions reach higher levels of escalation and cover broader swathes of the economy. Established financial institutions are likely to exit the market in order to avoid exposure to sanctions, and sanctions can also result in broad macroeconomic effects, such as rampant inflation.⁴ The Department of the Treasury has taken an important

⁴Rice, Tara, and von Peter, Goetz, and Boar, Codruta, “On the Global Retreat of Correspondent Banks” (*BIS Quarterly Review*, March 01, 2020), <https://www.bis.org/publ/qtrpdf/r-qtr2003g.htm>; Esfandiyar Batmanghelidj and Erica Moret, “The Hidden Toll of Sanctions: Why Washington Must Reckon With the Devastating Inflation Its Policies Cause”, *Foreign Affairs*,

step to address humanitarian concern by establishing an office dedicated to assessing the impact of sanctions. Analytic efforts, such as those carried out by this office, are important to project potential humanitarian impacts, as well as to monitor unanticipated effects of the sanctions. Congress should support efforts at Treasury and elsewhere in the U.S. Government to anticipate and monitor potential humanitarian impacts.

Additionally, engagement with the humanitarian community is key to understanding and addressing the impact of sanctions on marginalized communities. Humanitarian groups regularly report that it is difficult to provide humanitarian support within a heavily sanctioned jurisdiction. General licenses that explicitly permit the provision of humanitarian aid, as well as food and medicine, can address part of this problem. For example, the United States exempted food and medicine from its sanctions and export controls in the Russia case. Policymakers must remain in dialogue with humanitarian groups to understand the practical constraints that sanctions place on their operations as well as humanitarian conditions on the ground.

Q.3. Given that the People’s Republic of China is heavily subsidizing its domestic solar manufacturing industry and flooding the market with solar panels at lower prices than American competitors can offer,⁵ what steps can Congress and the Administration take to maximize investment in affordable clean energy and incentivize domestic production?

A.3. Investments in domestic manufacturing capacity are critical to ensure that the United States has a balanced clean energy policy that creates demand for clean energy technologies while also ensuring that the supply of these technologies is secure and reliable. Incentivizing domestic production can take a range of forms, such as the tax incentives included in the Inflation Reduction Act (IRA), funding for clean energy supply chains provided under Defense Production Act (DPA) authorities, or establishment of new financing mechanisms (e.g., the Industrial Finance Corporation) to fund projects that are under-valued by the private sector. The United States may wish to consider trade remedies, such as anti-dumping or countervailing duties, to address the nonmarket practices and unfair subsidies of the People’s Republic of China (PRC). However, these remedies have traditionally been slow to deliver relief and can result in unintended consequences, such as commercial harm to U.S. installers of solar energy who rely on lower cost goods from China.⁶

The United States must also ensure that the domestic market can support clean energy investments. The United States must make investments in a clean energy workforce, building the skills necessary for a clean energy economy while ensuring that workers

January 17, 2022, <https://www.foreignaffairs.com/articles/world/2022-01-17/hidden-toll-sanctions>.

⁵Ana Swanson and Kim Tankersley, “Flush With Investment, New U.S. Factories Face a Familiar Challenge”, *The New York Times*, January 15, 2024, <https://www.nytimes.com/2024/01/15/business/economy/china-electric-cars-chips-solar.html>.

⁶Nichola Groom, “U.S. Places Tariffs on Some Big Solar Companies for Dodging China Duties”, *Reuters*, August 18, 2023, <https://www.reuters.com/sustainability/us-slaps-tariffs-some-big-solar-companies-dodging-china-duties-2023-08-18/>.

benefit from a transition to clean energy technologies.⁷ As the climate transition shifts the composition of jobs in the economy, the U.S. Government must focus on reskilling and retraining workers who may be negatively impacted (e.g., workers at factories making internal combustion engine cars). In the electric vehicle space, investments in technology must be paired with supporting infrastructure. Early efforts to develop national electric vehicle charging infrastructure have been slow, which may have negative repercussions for adoption and consumer demand.⁸

RESPONSES TO WRITTEN QUESTIONS OF CHAIR BROWN FROM JAMIL N. JAFFER

Q.1. In previous testimony to the House of Representatives, you cited the Export-Import Bank's China and Transformational Exports Program as an example of how Federal financing for American industry can help "fill the gap that Chinese economic coercion creates." Congress directed EXIM to use the CTEP program to prioritize financing for American exports in ten critical areas, such as artificial intelligence, renewable energy and energy storage, wireless communications, and semiconductors.

We have heard that EXIM's ability to provide financing to emerging industries is partially constrained because of the rules established by Congress for the Bank's default rate. While EXIM can provide financing for American exporters in emerging industries, the Bank has to be more conservative in its lending practices to ensure stability in its default rate. If the Bank's traditionally low default rate increases too much, the Bank essentially loses the ability to provide any new financing—not only making it harder for us to compete with China but also limiting our ability to support U.S. exporters, including small businesses looking to grow their global market share.

Should our Committee look at how Congress could help EXIM provide more financing to American companies that face Chinese competition in key sectors?

A.1. There is no question that there is significant value in the Senate Committee on Banking, Housing, and Urban Affairs looking at how the Committee—and Congress at large—might be able to help the Export-Import Bank of the United States (EXIM) provide more financing to American companies that are competing with Chinese companies in key sectors, including the ten transformational sectors identified in the China and Transformational Exports Program (CTEP). Such support is vital to allowing U.S. companies to be fully competitive in areas such as artificial intelligence, biotechnology, biomedical capabilities, wireless communications, renewable energy, semiconductors, financial technology, water treatment and sanitation, and high-performance computing, as well as underlying capabilities like critical minerals mining and processing. Ensuring that American companies are not only competitive

⁷ Jack Ewing, "Battle Over Electric Vehicles Is Central to Auto Strike", *The New York Times*, September 16, 2023, <https://www.nytimes.com/2023/09/16/business/electric-vehicles-uaw-gm-ford-stellantis.html>.

⁸ James Bikales, "Congress Provided \$7.5B for Electric Vehicle Chargers. Built So Far: Zero". *Politico*, December 5, 2023, <https://www.politico.com/news/2023/12/05/congress-ev-chargers-billions-00129996>.

but win these opportunities abroad in in the economic and national security interest of our Nation.

As you know, in September 2023, the EXIM Office of Inspector General issued a report which found that “EXIM’s 2 percent default rate cap, a statutory requirement, is unique among OECD [Export Credit Agencies] and discourages staff from taking risks and meeting other Congressional Mandates.”¹ Given the critical importance of CTEP, at a minimum, Congress ought fully exclude CTEP transactions from the statutory default rate calculation where such transactions are approved by the EXIM Board of Directors.

In addition, as you may recall in 2021, the EXIM Advisory Committee Chairman, former Congressman Stevan Pearce (R-NM), sent EXIM’s 2020 Report to the U.S. Congress on Global Export Competition to Congress and recommended, with respect to CTEP, that “Congress fully resource this significant new mandate which also has national security components” and that “Congress consider expanding EXIM’s authority to support defense articles and services and review how foreign ECAs support such exports.”² I support these recommendations. In addition, the Committee might review CTEP’s current staffing and budget and take action to provide the full resources necessary to fulfill the CTEP mandate provided by Congress in its 2019 reauthorization of EXIM.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR CORTEZ MASTO FROM JAMIL N. JAFFER

Q.1. This week the International Monetary Fund (IMF) released a new analysis that examines the potential impacts of AI on the global labor market and says that AI will affect almost 40 percent of global jobs. Do you generally agree with this analysis, and if so, how do you think the productivity gains from AI compared to the jobs losses from the technology will impact the specific competition between the U.S. and China?

A.1. There is no question that the advent and widescale adoption of artificial intelligence will have a significant impact on jobs globally, however it remains unclear whether this will result in a net gain or loss of jobs and whether the productivity gains will outstrip any net loss should there be one.¹ The IMF’s analysis itself notes that “AI will expand economies’ production frontiers and will lead to reallocations between labor and capital while triggering potentially profound changes in many jobs and sectors” and that “AI

¹ See EXIM Office of the Inspector General, “Comparative Analysis of U.S. and OECD Arrangement Export Credit Agencies”, OIG-EV-23-04, at 24 (Sept. 29, 2023), available online at <https://www.oversight.gov/sites/default/files/oig-reports/EIB/EXIM-OIGECA-EvaluationOIG-EV-23-04FINAL.pdf>.

² See Export-Import Bank of the United States, “2020 Report to the U.S. Congress on Global Export Competition”, at 8–9 (July 2021), available online at <https://img.exim.gov/s3fs-public/reports/competitiveness-reports/2020/EXIM-2020-CompetitivenessReport-Web-Ready-Single%20pages.pdf>.

³ See Mauro Cazzinga, et al., “Gen-AI: Artificial Intelligence and the Future of Work”, at 2, International Monetary Fund (Jan. 14, 2024), available online at <https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2024/01/14/Gen-AI-Artificial-Intelligence-and-the-Future-of-Work-542379?cid=bl-com-SDNEA2024001> (“Artificial intelligence (AI) is set to profoundly change the global economy, with some commentators seeing it as akin to a new industrial revolution. Its consequences for economies and societies remain hard to foresee. This is especially evident in the context of labor markets, where AI promises to increase productivity while threatening to replace humans in some jobs and to complement them in others.”)

[also] offers unprecedented opportunities for solving complex problems and improving the accuracy of predictions, enhancing decision-making, boosting economic growth, and improving lives.”² At the same time, the IMF notes that “precisely because of its vast and flexible applicability in numerous domains, the implications for economies and societies are uncertain.”³

Overall, however, the IMG assesses that “[o]wing to capital deepening and a productivity surge, AI adoption is expected to boost total income” and that “[i]f AI strongly complements human labor in certain occupations and the productivity gains are sufficiently large, higher growth and labor demand could more than compensate for the partial replacement of labor tasks by AI, and incomes could increase along most of the income distribution.”⁴

There is strong evidence from prior revolutions that significant advances in technology, systems, and processes result in long-term economic gains in societies that are able to adopt the new technologies and take advantage of them.⁵ Given this, there is little doubt in my mind that the United States will be net advantaged by the advent of artificial intelligence if we are able to maintain or expand our current technology lead with respect to China.

Q.2. How do you envision each country’s approach to AI expansion may account for different labor market results?

A.2. It is hard to assess at this time the impact of each country’s approach to AI expansion on the labor markets.⁶ The IMF’s analysis indicates that “[t]he impact of AI is also likely to differ significantly across countries at different levels of development or with different economic structures.”⁷ Specifically, the IMF notes that “[a]dvanced economies, with their mature industries and service-driven economies, typically have a higher concentration of jobs in sectors that require complex cognitive tasks . . . [and] therefore [are] both more susceptible to, yet better positioned to benefit from, AI innovations.”⁸ At the same time, the IMF also notes that “emerging market and developing economies, often still reliant on manual labor and traditional industries, may initially face fewer AI-induced disruptions . . . [but] these economies may also miss

²See id. at 3.

³Id.

⁴Id. at 2.

⁵See, e.g., Diego Comin and Bart Hobijn, “An Exploration of Technology Diffusion”, at 4, 21–25, Harvard Business School Working Paper No. 08-093 (Apr. 2008), available online at <https://www.hbs.edu/ris/Publication%20Files/08-093—097fb722-e6dd-466d-aa1a-29733fa92757.pdf>

(“The remarkable development records of Japan in the second half of the Nineteenth Century and the first half of the Twentieth Century and of the, so-called, East Asian Tigers in the second half of the Twentieth Century all coincided with a catch-up in the range of technologies used with respect to industrialized countries. All these development miracles involved a substantial reduction of the technology adoption lags in these countries relative to those in (other) OECD countries.”); see, also, Darrell M. West, “Technology and the Innovation Economy”, at 1, Center for Technology Innovation, Brookings Institution (Oct. 19, 2011), available online at <https://www.brookings.edu/wp-content/uploads/2016/06/1019-technology-innovation-west.pdf> (noting that “[i]nnovation and entrepreneurship are crucial for long-term economic development” and that “[r]esearchers have found a link between technology innovation and national economic prosperity”); Noshua Watson, “How Technology Spreads”, *The Digest*, National Bureau of Economic Research (July 2001), available online at <https://www.nber.org/digest/jul01/how-technology-spreads> (“The adoption of new technology is essential to long-term macroeconomic growth.”).

⁶Id.

⁷See Cazzinga, et al., “Gen-AI”, supra n. 3, at 4.

⁸Id.

out on early AI-driven productivity gains, given their lack of infrastructure and a skilled workforce.”⁹

Regardless, if one accepts the assessment above that the U.S. will be net advantaged by broad adoption of AI capabilities if it maintains or expands the technological edge it currently enjoys, based on the historic productive gains as a result of rapid technology adoption, then accelerating AI expansion at home is in the economic and national security interests of the United States.

**RESPONSES TO WRITTEN QUESTIONS OF
SENATOR CORTEZ MASTO FROM LINDSAY GORMAN**

Q.1. This week the International Monetary Fund (IMF) released a new analysis that examines the potential impacts of AI on the global labor market and says that AI will affect almost 40 percent of global jobs. Do you generally agree with this analysis, and if so, how do you think the productivity gains from AI compared to the jobs losses from the technology will impact the specific competition between the U.S. and China?

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

Q.2. How do you envision each country’s approach to AI expansion may account for different labor market results?

A.2. Response not received in time for publication.

**RESPONSES TO WRITTEN QUESTIONS OF
SENATOR VAN HOLLEN FROM LINDSAY GORMAN**

Q.1. You testified to the importance of collaboration to help strengthen our competition strategy, calling for better coordination among Federal agencies and for improved multilateral cooperation with our partners and allies.

In what specific ways should we better organize and leverage the tools at our disposal to promote multilateral cooperation to more effectively advance our competition strategy?

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

Q.2. While it is preferable to secure multilateral cooperation through voluntary participation, under what circumstances should the United States use secondary sanctions to achieve our goals?

A.2. Response not received in time for publication.

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR WARNOCK
FROM LINDSAY GORMAN**

Q.1. You have previously noted that the CHIPS and Science Act (Pub. L. 117-167) is “an excellent start in reversing the chronic public underfunding of U.S. research and development.”¹ How can the United States leverage our strengths and build upon the suc-

⁹Id.

¹“Commanding Heights: Ensuring U.S. Leadership in the Critical and Emerging Technologies of the 21st Century”, The House Select Committee on the Chinese Communist Party (July 26, 2023), Prepared Testimony from Lindsay Gorman, <https://selectcommitteeontheccp.house.gov/committee-activity/hearings/hearing-notice-commanding-heights-ensuring-us-leadership-critical-and>.

cesses of the CHIPS and Science Act to better counter China's current technology investment strategy?

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

Q.2. The People's Republic of China has spent hundreds of billions of dollars building up its solar industry and today, it controls more than 80 percent of the share in all the manufacturing stages of solar panels.² Given that China is heavily subsidizing its domestic solar manufacturing industry and flooding the market with solar panels at lower prices than American competitors can offer,³ what steps can Congress and the Administration take to maximize investment in affordable clean energy and incentivize domestic production?

A.2. Response not received in time for publication.

²Special Report on Solar PV Global Supply Chains, International Energy Agency (2022), <https://www.iea.org/reports/solar-pv-global-supply-chains>.

³Id.