S. HRG. 115–213

CFIUS REFORM: EXAMINING THE ESSENTIAL ELEMENTS

HEARING

BEFORE THE

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

ON

EXAMINING THE ESSENTIAL NATIONAL SECURITY ELEMENTS UNDERLYING A COMPREHENSIVE PROPOSAL TO REFORM THE REVIEW PROCESS USED BY THE COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES (CFIUS)

JANUARY 18, 2018

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

Available at: http://www.govinfo.gov/

U.S. GOVERNMENT PUBLISHING OFFICE

29–914 PDF WASHINGTON : 2019

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

MIKE CRAPO, Idaho, *Chairman*

RICHARD C. SHELBY, Alabama	SHERROD BROWN, Ohio
BOB CORKER, Tennessee	JACK REED, Rhode Island
PATRICK J. TOOMEY, Pennsylvania	ROBERT MENENDEZ, New Jersey
DEAN HELLER, Nevada	JON TESTER, Montana
TIM SCOTT, South Carolina	MARK R. WARNER, Virginia
BEN SASSE, Nebraska	ELIZABETH WARREN, Massachusetts
TOM COTTON, Arkansas	HEIDI HEITKAMP, North Dakota
MIKE ROUNDS, South Dakota	JOE DONNELLY, Indiana
DAVID PERDUE, Georgia	BRIAN SCHATZ, Hawaii
THOM TILLIS, North Carolina	CHRIS VAN HOLLEN, Maryland
JOHN KENNEDY, Louisiana	CATHERINE CORTEZ MASTO, Nevada
JERRY MORAN, Kansas	DOUG JONES, Alabama

GREGG RICHARD, *Staff Director*
MARK POWDEN, *Democratic Staff Director*

ELAD ROISMAN, *Chief Counsel*
JOHN V. O'HARA, *Chief Counsel for National Security Policy*
KRISTINE JOHNSON, *Economist*

ELISHA TUKU, *Democratic Chief Counsel*
COLIN MCGINNIS, *Democratic Policy Director*

DAWN RATLIFF, *Chief Clerk*
JAMES GUILIANO, *Hearing Clerk*
SHELVIN SIMMONS, *IT Director*
JIM CROWELL, *Editor*

C O N T E N T S

THURSDAY, JANUARY 18, 2018

	Page
Opening statement of Chairman Crapo	3
Prepared statement	33
Opening statements, comments, or prepared statements of:	
Senator Brown	5

WITNESSES

John Cornyn, a U.S. Senator from the State of Texas	1
Prepared statement	34
Dianne Feinstein, a U.S. Senator from the State of California	
Prepared statement	37
Christopher Padilla, Vice President for Government and Regulatory Affairs, IBM Corporation; and Former Under Secretary for International Trade, Department of Commerce	7
Prepared statement	38
Responses to written questions of:	
Chairman Crapo	67
Senator Cotton	68
Senator Menendez	70
Senator Warner	71
Senator Cortez Masto	72
Scott Kupor, Managing Partner, Andreessen Horowitz, and Chair, National Venture Capital Association	9
Prepared statement	43
Responses to written questions of:	
Chairman Crapo	73
Senator Menendez	75
Senator Warner	76
Senator Cortez Masto	77
Gary Clyde Hufbauer, Ph.D., Reginald Jones Senior Fellow, Peterson Institute for International Economics	11
Prepared statement	53
Responses to written questions of:	
Chairman Crapo	79
Senator Menendez	79
Senator Warner	80
Senator Cortez Masto	81
James Mulvenon, Ph.D., General Manager, Special Programs Division, SOS International	12
Prepared statement	56
Responses to written questions of:	
Chairman Crapo	82
Senator Menendez	82
Senator Warner	83
Senator Cortez Masto	83

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

FIRRMA-related documents—summaries, letters, quotes, and background papers—submitted by Senator Cornyn	85
Prepared statement of the Rail Security Alliance	125

CFIUS REFORM: EXAMINING THE ESSENTIAL ELEMENTS

THURSDAY, JANUARY 18, 2018

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

The Committee met at 9:47 a.m. in room SD–538, Dirksen Senate Office Building, Hon. Mike Crapo, Chairman of the Committee, presiding.

Chairman CRAPO. This hearing will come to order.

This morning, we are going to go immediately to Senator Cornyn for his statement, and then we will return back to Senator Brown and myself to give opening statements and then go to the witnesses.

So, Senator Cornyn, without any further ado, you may begin your statement at any time.

STATEMENT OF JOHN CORNYN, A U.S. SENATOR FROM THE STATE OF TEXAS

Senator CORNYN. Thank you, Mr. Chairman and Ranking Member Brown and Members of the Committee. I appreciate your holding this hearing to consider mine and Senator Feinstein's proposal called the Foreign Investment Risk Review Modernization Act, or FIRRMA.

I will make abbreviated remarks, and I would ask consent, Mr. Chairman, to have my full testimony put in the record along with a written statement by Senator Feinstein who could not be here because she is Ranking on Judiciary and has a conflicting engagement.

Senator CORNYN. Senator Feinstein and I spent months working on FIRRMA based in part on troubling information we both regularly hear as members of the Senate Select Committee on Intelligence. The bill takes a targeted approach at addressing specific national security problems while aiming not to unnecessarily chill foreign investment. I support foreign investment in the United States.

I would like to take a moment to highlight the list of people who we have worked with, we have consulted with to try to improve this legislation and who have announced their support for it. It includes, of course, Members of the Committee like Senator Scott who introduced this bill with us, and it includes current and former U.S. national security leaders like Secretary of Defense James Mattis; Secretary of Treasury Steve Mnuchin; Attorney General Jeff Sessions; Admiral Harry Harris, Commander of U.S. Pacific

Command; former Secretaries of Defense like Donald Rumsfeld and Bill Perry; former Homeland Security Secretary Michael Chertoff; former DNI, Director of National Intelligence, Admiral Dennis Blair; and other distinguished retired four-star generals and admirals.

It also includes industry players such as Ericsson, Oracle, and several other companies and trade groups from across the country.

Mr. Chairman, I would ask consent to submit for the record their letters and quotes as well as several summary and background documents on FIRRMA.

Chairman CRAPO. Without objection.

Senator CORNYN. The context for this legislation is important, and it is easily misunderstood, so I want to hopefully correct some misconceptions. The context for this legislation is about China. I am an ardent supporter of free trade, and I strongly support foreign investment in the United States, consistent with the protection of our national security. China, however, has significantly altered the threat landscape for the United States.

General Joe Dunford, Chairman of the Joint Chiefs of Staff, says that by 2025, China will pose the greatest threat to U.S. national security of any other nation. China poses a threat unlike anything the United States has ever faced before—a powerful economy with coercive, state-driven industrial policies that undermine the free market, married up with an aggressive military modernization and the intent to dominate not only its own region but potentially beyond.

China uses both legal and illegal means to turn our own technology and knowhow against us and erase our national security advantage. One of these tools is investment, which China has weaponized to vacuum up U.S. industrial capabilities in dual-use technologies.

Unfortunately, the jurisdiction of the Committee on Foreign Investment in the United States that reviews such transactions is limited, and China has studied the law and found gaps to exploit. To circumvent CFIUS review, China pressures U.S. companies into arrangements like joint ventures, coercing them into sharing their capabilities and their intellectual property and enabling Chinese companies to acquire that and then the knowhow that goes along with it and replicate them on Chinese soil, which undermines our defense industrial base.

China has been able to exploit minority position investments in early stage technology companies to gain access to cutting-edge intellectual property as well as trade secrets and key personnel. The Chinese have figured out which dual-use emerging technologies are still in the cradle, so to speak, and not yet subject to export controls.

I want to quickly debunk three flawed arguments advanced by some who have opposed our efforts. First, they say the bill represents regulatory overreach, which really misses the point. CFIUS is not a normal regulator by any means. It is a part of our national security apparatus, and the Federal Government has no higher duty—I would argue no American has a higher duty than to protect and to maintain our national security.

Second, opponents claim that the export control system can already address these national security risks. Well, under FIRRMA, export controls would remain the first line of defense when it comes to technology transfers, but that system has inherent limitations, so we need a second line of defense. And CFIUS and export controls are designed to be interactive and complementary and not mutually exclusive.

What is more, FIRRMA includes safeguards to ensure that CFIUS would review transactions only when necessary. Many transactions would be exempted where there are other authorities, such as export controls that adequately address national security risks.

CFIUS would also create a safe list of certain allied countries for which these new types of transactions would be exempt.

Third, some opponents argue that FIRRMA will flood CFIUS with too many transactions, seemingly questioning whether addressing real national security threats is worth the time and expense. Well, it is, and I am fully committed to securing the necessary resources working together with my colleagues because this is a national security priority.

So, in closing, Mr. Chairman, I want to ask those who perhaps are skeptical of what we are trying to do here to withhold judgment until you have heard the front-line perspectives of key member agencies of CFIUS. The time, I believe, to modernize CFIUS is now. Our adversaries and rivals around the world are on the march, and they are vacuuming up our cutting-edge dual-use technology, which not only cuts our technological advantage when it comes to national security but undermines our industrial base here at home, as I have said.

The time to modernize CFIUS is now, and we must not allow ourselves to be the frog in the pot of boiling water, so to speak. So I urge you to advance this bill for the sake of our long-term national security.

Thank you, Mr. Chairman, I really appreciate the opportunity to present these remarks and the cooperation that you and others on the Committee and other colleagues have shown in trying to address this vital national security issue.

Chairman CRAPO. Thank you, Senator, Cornyn. We appreciate both you and Senator Feinstein bringing this critical issue to us and the work that you have put into it, and we appreciate your testimony here today.

You are obviously facing a pretty busy schedule and are free to leave at any time you wish. Thank you, and thanks again for bringing this to us.

OPENING STATEMENT OF CHAIRMAN MIKE CRAPO

Chairman CRAPO. Today the Committee will begin to evaluate the essential national security elements underlying a comprehensive proposal to reform the review process used by the Committee on Foreign Investment in the United States, or CFIUS.

Again, thanks go to Senators Feinstein and Cornyn for their testimony and work on their bipartisan Foreign Investment Risk Review Modernization Act of 2017.

The bill was first introduced by Senators Cornyn and Feinstein on November 8th to modernize and strengthen CFIUS to more effectively guard against the risk to the national security of the United States posed by certain types of foreign investment.

The Senators and their staff have worked well over a year with concerned national security officials, the Treasury Department, and various affected industry representatives.

This comprehensive bill could be the first update to the body of the CFIUS law in more than a decade. It would expand the reach of current law in a number of respects, while codifying some current administrative practices, and result in significant changes to jurisdiction, process, and enforcement.

A study produced for the Pentagon's DIUx unit, which enlists startups to find solutions for the military's most advanced technology-related requirements, is credited as being the catalyst for much of the impetus behind this CFIUS reform.

The DIUx study highlights the problems arising from the fact that the U.S. Government does not currently monitor or restrict venture investing nor stop potential transfers of what is known variously as early stage, foundational, or critical technology know-how, particularly with regard to certain types of Chinese investment in the United States.

Today's hearing also draws witnesses from one perspective of the private sector that is concerned not only with inbound investment but also outbound transactions and from the venture capitalists that support American innovation.

We are also joined by two long-time CFIUS analysts with particular expertise in regard to China's economy, its trade practices, and national security objectives.

The Committee will benefit from learning more about the types and numbers of transactions that may be circumventing CFIUS and if any are believed to have already transferred critical technology.

Many of us are interested in learning more about the ways China acquires U.S. technology and which improvements to the current system are warranted, particularly with regard to those investments that fall short of a foreign person's actual ownership or control.

We are also interested in the issue of emergent critical technology and the witnesses' input on how it would be defined and applied by CFIUS.

Additionally, we hope to hear more on the impact on U.S.-based multinational corporations as a result of CFIUS unilaterally restricting U.S. outward investment and associated technology and whether U.S. companies would lose the ability to compete to allied companies or others in third-country markets.

It is also important to study the question of necessary resources for any proposed reform to CFIUS. While CFIUS certified about 260 applications last year, the Committee looks forward to testimony on the changes contemplated by S. 2098 and their impact on the number of reviews, staff needs and resources going forward, and the impact that, in turn, would have on U.S. national security if the resources fell short.

CFIUS is but one leg of a triad that secures national security-related technology and the defense industrial base. The other two are the U.S. export control regime and Federal investment itself in research and development that keeps the industrial base resilient and innovative.

The Committee must be mindful that in pursuing its mandate to assure the national security interests of the United States under CFIUS that it not create a situation where it chills a wide range of commercial activities that have traditionally been controlled through export control laws.

The United States is both the world's largest foreign direct investor and beneficiary of foreign direct investment, and it ranks among the most favorable destinations for FDI which plays an important role in not only the U.S. economy but specifically in the innovation of its industrial base and, therefore, its national security.

It is clear that the current CFIUS system is itself under stress. Moving forward, the Committee must prepare itself to thoughtfully consider all of the recommendations made by S. 2098 and other CFIUS legislation, with the full awareness of the national security and economic stakes at heart.

It is a new world. The laws, regulations, and policies currently exercised by CFIUS may no longer protect U.S. technology from illicit transfers as they did in the past.

We must work together as a Congress first to assure the national security of the United States by granting the Administration all the authority it needs to confront this growing threat, but then not exceed that grant to the detriment of maintaining a free, fair, and open U.S. investment policy.

Senator Brown.

STATEMENT OF SENATOR SHERROD BROWN

Senator BROWN. Well, thank you, Chairman Crapo, and thank you to the witnesses for joining us. I comment Senators Cornyn and Feinstein for their work on this issue.

A dozen years ago, I was serving in the House of Representatives when we learned the Bush administration had signed off on the sale of the operations at more than 20 U.S. ports, including major ones from New York and New Jersey to New Orleans, to Dubai Ports World.

Congress responded the next year by adopting FINSA, the Foreign Investment and National Security Act, to give our Government a greater ability to respond to foreign investment that could pose a threat to national security and to protect critical infrastructure.

In the intervening years, the interagency group that implements the law, the Committee on Foreign Investment in the United States has quietly worked to try to ensure that foreign purchases of assets in the United States does not undermine our national security—obviously not an easy task, as our witnesses will describe, our adversaries are constantly working to narrow the gaps between our capabilities and theirs, through legitimate and illegitimate means.

Over the past decade, we have seen China become more aggressive. The evidence stretches from the OPM servers to the South

China Sea. We know that CFIUS has a limited mandate, and we know the distinction between economic security and national security is not an easy one to make.

Foreign direct investment can be a real positive for our country. It was a French company, for example, that built the first rolling mill in Youngstown, Ohio, in decades.

But today we will hear testimony that some foreign investors are not interested in capturing market share in auto or oil country tubular goods or any other industry. Instead, they seek to capture the intellectual property of leading edge technology companies in our country for their home country's military uses.

We attempt today to prevent this type of technology transfer through a system of multilateral and unilateral export controls. This system, a product of the cold war, identifies dual-use products, technology, and software that may not be exported.

The question is, is this approach sufficient, or do we need to intervene at an earlier stage of product or technology development to prevent the building blocks of the next generation of advances from being expropriated by foreign investors?

I mentioned at the beginning of my remarks the failure of the Bush administration to block the sale of our port operations to a company from the UAE, but this is not a partisan issue. The Clinton administration agreed to China's accession to the WTO. A number of us opposed that. They agreed to that accession. The Obama administration refused to take action in the face of China's manipulation of its currency.

Some of our witnesses today will speak to the benefits of trade liberalization, but it is hard to maintain a bilateral trading partnership when one party is abiding by the rules and the other is not.

When China joined the WTO in 18 years, 17 years ago, it agreed to remove market barriers for foreign companies and to comply with international trade standards that are intended to create a worldwide level playing field. Unfortunately, as we know and we feel all too often, China has not lived up to many of these commitments. That country continues to use nontariff barriers to block foreign producers from entering its market. Chinese state-owned enterprises, such as those in the steel sector, receive extensive subsidies that allow them to compete with no consideration of market forces. It can be energy. It can be land. It can be capital. It can be other kinds of inputs. As a result, they flood the global market with steel products and make it much harder for U.S. companies and workers to compete.

I do not think CFIUS can or should bear the burden of trying to bring about a fair trading relationship with China. That is not its job. That is not its intent. It has its hands full trying to police the national security threats we face from that country and others.

But neither should we sit idle. The vast majority of foreign investment in the United States falls, of course, outside the scope of CFIUS. But we do not have a way to review that investment to make sure it is in our economic interests.

I have introduced legislation with Senator Grassley—both of us are members of the Finance Committee—called the Foreign Investment Review Act that would require the Secretary of Commerce to

review certain foreign investments, particularly those made by state-owned-enterprises, to make sure they are in the long-term, strategic interests, economic and otherwise, of the United States.

I agree we should update CFIUS to respond to the challenges we face. It is equally important now, Mr. Chairman, that we recognize that the same practices that undermine our national security, can pose a threat to our economic security as a Nation as well.

Thank you.

Chairman CRAPO. Thank you, Senator Brown.

We will now move to our witnesses and their testimony. We have with us four excellent witnesses today, and in the order of your testimony, they will be the Honorable Christopher Padilla, Vice President for Government and Regulatory Affairs at IBM Corporation, and former Under Secretary for International Trade at the U.S. Department of Commerce. Second will be Mr. Scott Kupor, Managing Partner at Andreessen Horowitz and Chairman of the Board of National Venture Capital Association. Next would be Dr. Gary Clyde Hufbauer, the Reginal Jones Senior Fellow at the Peterson Institute for International Economics; and finally, Dr. James Mulvenon.

Did I get that pronounced right? Close?

Mr. MULVENON. Mulvenon.

Chairman CRAPO. Mulvenon? All right. Thank you for that.

Dr. James Mulvenon, the General Manager at the Special Programs Division of SOS International.

Gentlemen, we appreciate you being with us today and your bringing your expertise to assist us with this issue. We will proceed in the order that I introduced you. I remind you that we ask you to keep your oral remarks to 5 minutes, so we have time for questions and answers. And I again remind our Senators to do the same when their turn for questions comes.

Thank you. And Mr. Padilla.

STATEMENT OF CHRISTOPHER PADILLA, VICE PRESIDENT FOR GOVERNMENT AND REGULATORY AFFAIRS, IBM CORPORATION; AND FORMER UNDER SECRETARY FOR INTERNATIONAL TRADE, DEPARTMENT OF COMMERCE

Mr. PADILLA. Thank you, Mr. Chairman.

During the Administration of President George W. Bush, I served as Assistant Secretary of Commerce responsible for export controls in addition to my role as Under Secretary, and in that and other Administration roles, I was a senior sub-Cabinet official on CFIUS.

Interestingly, the last major expansion of export controls focused on China, which looked at Chinese military end users, bears my signature. It was signed in June of 2007 when I served as Assistant Secretary for Export Administration.

In my role at IBM, I have been involved in two transactions that were reviewed and approved by CFIUS, and I am responsible for the company's compliance with export controls. And my comments will draw on these experiences.

I would like to focus my remarks on the FIRRMA bill discussed by Senator Cornyn this morning, and let me start by saying that FIRRMA contains, I think, some important reforms that IBM supports—to expand the ability of CFIUS, to examine certain inbound

investments, plugging gaps that do exist in its jurisdiction. These include expanding the ability of the committee to look at a wider range of inbound investment, taking measures to prevent the evasion of CFIUS, and ensuring senior-level review of cases. We also support increasing resources for the committee.

But the problem with FIRRMA, Mr. Chairman—and it is a big one—is that the bill does something else. It would drastically expand the committee's mandate beyond examining inbound investment. For the first time ever, CFIUS would also review outbound international transactions, including thousands of nonsensitive sales, IP technology transfer deals, even with friendly nations, and this is a serious flaw in the bill. It would duplicate and undermine the existing U.S. export control system, would result in a flood of cases that would overwhelm CFIUS, and could constitute the largest unilateral trade controls imposed by the United States in many decades.

Controlling sensitive technology works best when it is done internationally in cooperation with allies. A technology control system that only unilaterally stops U.S. firms from doing business abroad will not advance security interests if it simply hands out markets to foreign competitors, many of whom are equally adept in advanced technology, yet this is precisely what FIRRMA would do.

As drafted, the bill would impose a very onerous and entirely unilateral set of restrictions on overseas transactions involving the contribution, vaguely defined, of technology, IP, and associated support through any—I emphasize "any"—type of arrangement.

This could capture under CFIUS things like the sale of a computer server to a bank in Singapore, the licensing of a database to a pharmaceutical company in Switzerland. Even routine licensing of trademarks could require CFIUS review. Saying, as the bill does, that ordinary customer relationships are excluded does not narrow the bill because that term is also left to regulators to define. With such a broad reach, the CFIUS caseload would skyrocket from about 250 cases a year now, which is already a record, to many thousands or even tens of thousands.

Now, I know as Senator Cornyn said, one of the issues driving FIRRMA is a concern that the export control system has not kept up to date, but the answer to that is not to abandon export controls and dump everything on to CFIUS, layering another bureaucracy on top of foreign commerce. I think the better answer is that there is existing regulatory authority to impose new export controls quickly over time in partnership with our allies. This can be done under current rules already on the books.

So the authority is there, but the control lists do need a refresh. A GAO report found in February 2015 that the Defense Department was no longer updating or even using the Militarily Critical Technologies List, which was established in statute by Congress to keep export controls up to date.

FIRRMA would not correct this problem and could make it worse. Under FIRRMA, the Government would define a vague new list of technologies, even though it is not using the one it is already supposed to keep, and then wait until something pops up in a transaction review. We might then try to stop it in a haphazard

and scattershot way on a deal-by-deal basis, but that would be totally unilateral.

Casting a huge regulatory net over business and applying a test of, essentially, "We will know it when we see it" would be very damaging to both competitiveness and security. I think the answer, Mr. Chairman, is not to turn CFIUS into a super export control agency. Instead, Congress and this Committee should use its oversight authority to demand updates, to export controls, ideally in cooperation with our allies to reflect current technology. If you do that combined with a slimmed-down FIRRMA bill that does plug some gaps in the ability of CFIUS to look at inbound investment, I think that would be the best approach for our economy and for our national security.

Thank you, Mr. Chairman.

Chairman CRAPO. Thank you, Mr. Padilla.

Mr. Kupor.

STATEMENT OF SCOTT KUPOR, MANAGING PARTNER, ANDREESSEN HOROWITZ, AND CHAIR, NATIONAL VENTURE CAPITAL ASSOCIATION

Mr. KUPOR. Chairman Crapo, Ranking Member Brown, Members of the Committee, thank you again for the time today and the opportunity to testify regarding the Foreign Investment Risk Review Modernization Act. My name is Scott Kupor and I am the Managing Partner of Andreessen Horowitz. We are a venture capital firm that has partnered with many innovative technology companies. I am here today in my capacity, though, as the Chairman of the National Venture Capital Association.

The venture capital industry shares the goals of this Committee and FIRRMA's authors to protect U.S. innovation and ensure that technology is not used to harm our competitiveness or security. At the same time, we believe that Congress and the Administration should be mindful of the bill's potential impact on startups in the venture industry.

My testimony today will focus on the ways in which we think FIRRMA can be improved while still accomplishing its foundational goal.

First, I thought I would give you a quick background on what venture capitalists do and what it means to the overall economy and innovation. Venture capitalists like myself, we often are called general partners, or GPs, raise investment funds for a broad range of limited partners, or LPs. These are endowments, foundations, and pension plans, many of which are in your States.

We use this capital to invest in outstanding entrepreneurs with breakthrough ideas. The basic structure of a venture fund effectively protects the sensitive information of startups from disclosure of investors into the fund. We generally limit disclosure of limited partners to a very small amount, and most of that disclosure is related to valuation and accounting-related information to ensure that limited partners understand that is the current economic position is of the fund.

Limited partners do not have access to sensitive information, the concern of FIRRMA, and of course, they have no say in the investment decisions of the venture fund.

We hope, of course, that all the companies we invest in will succeed, but entrepreneurship is an inherently risky endeavor. It is worth the risk, though, because it is absolutely essential to our economy, with one study finding that young startups, mostly venture-backed, were responsible for almost all the 25 million net jobs created in the United States since 1977.

Increased interests in startups by other countries, though, has caused the share of global venture capital invested in the United States to fall from 90 percent to 54 percent in only a matter of 20 years. China is now the second largest destination in the world for venture capital, and in 2016, 6 of the 10 largest venture deals in the world occurred in China.

Entrepreneurship is now a global competition, and I strongly encourage policymakers to prioritize policies that will solidify our leadership position, be they regulatory, tax, or immigration related.

Against this backdrop, I would like to share our views on FIRRMA. I do believe FIRRMA is well-meaning legislation intended to deal with a very real challenge; however, as drafted, the legislation produces many questions for the venture industry that we believe should be clarified before the bill moves forward.

My written testimony goes into greater detail, but this morning, I thought I would highlight two key areas that we would offer for improvement.

First, we would recommend that FIRRMA be amended to clearly specify that U.S. venture funds with foreign limited partners are not implicated by the covered transaction definition, nor does a venture fund take on foreign personhood for purposes of FIRRMA merely because it has foreign limited partners.

As drafted, FIRRMA is ambiguous in its application to a venture capital fund with foreign limited partners. We are concerned that this ambiguity, especially when combined with a broad grant of rulemaking authority, will cause unnecessary confusion, cost, and burden for the venture capital industry, as venture firms will be left without a clear understanding of whether they must file with CFIUS and under what circumstances.

As I mentioned earlier, as a practical matter, information disclosure to limit partners is minimal and related largely to valuation and accounting-related information, and also, as you may know, most venture capitalists sit on the boards of directors of the companies in which they invest, and as a result, they owe duties of confidentiality directly to the shareholders of those companies.

Thus, to the extent a venture capitalist were aware of proprietary technology in use or being developed by the company, she would not be in a position to share that with limited partners. Hence, the risk of disclosure of proprietary intellectual property to a foreign LP, understandably of concern to Congress, is not a paramount risk in a typical venture capital fund structure.

Second, we would ask that FIRRMA be modified so it does not stifle foreign direct strategic investors that have become an important part of the U.S. startup financing and are increasingly investing alongside U.S. venture capital firms.

Specifically, FIRRMA should specify that CFIUS filing is not needed if the foreign strategic investor takes a de minimis stake in a startup, as in that case the foreign strategic investor is a

de facto passive investor, but might fear it does not meet the tightly drafted passive investment test.

In addition, we would ask that the passive investment test be broadened to reflect true passivity. These changes, we believe will maintain FIRRMA's intended effects, while avoiding serious issues for startups in the venture capital industry.

The bottom line is that U.S. venture capital in entrepreneurial companies are competing against a global set of investors and companies who would love to have the next set of breakthrough technologies developed in the countries of their origin. If we make it harder for foreign investment to come into U.S.-domiciled companies, that money will simply go to other countries that are more welcoming, and we risk losing the leading competitive position in innovation that the United States has long held. It is far better for the United States to continue to be the global financial center, where the benefits of economic and job growth stemming from technological innovation accrue to our citizens.

To conclude, our industry appreciates the interest the Committee and FIRRMA's authors have paid this important issue in national security. I hope my comments today have conveyed the modern startup investing ecosystem is complex, and care should be taken to ensure that it is not disrupted in a way that harms the ability of startups to grow. I also hope that we can all work together on policies that support the American entrepreneurial system.

Thank you again for the opportunity.

Chairman CRAPO. Thank you, Mr. Kupor.

Dr. Hufbauer.

STATEMENT OF GARY CLYDE HUFBAUER, PH.D., REGINALD JONES FELLOW, PETERSON INSTITUTE FOR INTERNATIONAL ECONOMICS

Mr. HUFBAUER. Thank you, Senator Crapo and Members of the Committee, and apologies for my hoarse throat. Many of my remarks overlap with what Chris Padilla said, so I will try to abbreviate them. And I appreciate, Senator Crapo, the balance you struck in your opening remarks between national security and economic progress.

Inward and outward foreign direct investment almost always benefit the U.S. economy, and the econometrics on this are just overwhelmingly strong. Therefore, in my view, the burden should be placed on those who would propose restrictions, and that is the way CFIUS has operated in the past.

As Chris said, S. 2098 and its House counterpart would significantly enlarge the CFIUS mandate to cover outward investment and technology transactions. I mean, that is an enormous expansion, and the bills would cast a skeptical eye, perhaps properly, toward investment into a firm based in an adversary nation. And that would seem to be China certainly, but also Russia, Iran, and I am sure there are others.

The new mandate, as both the previous speakers have said, could put U.S. multinationals at a disadvantage if they are competing with, let us say, British or European or Japanese multinationals who have the same technology because the United States would be prevented from selling, and the others could go ahead.

So with its enlarged mandate, CFIUS would need a much, much larger staff. I really want to emphasize that. To give them the mandate without the staff, everybody will be disappointed. As Chris said, the number of cases will jump from 200 to at least 1,000 and probably more.

And the way the enlarged mandate is written in the bill—maybe this is not how it would play out, but it seems to put the burden on private firms to show that the transaction will not reduce U.S. technological advantages in areas that are currently or might soon become subjects of national security concern.

So with those thoughts, I have just two recommendations. First, I think the new mandate should focus on adversaries, they should be named, and critical technology.

Now, we have just brilliant scientists in the National Academy and National Engineering Association and elsewhere, and they can identify these critical technologies. Let us name them, and it is not a one-for-all name. It is a rolling name.

And second, the bill ought to more explicitly take into account the availability of the technology in question from our allies. That would be Japan and Korea and Europe and Canada, and if we are going to block it to the adversaries, well, then we ought to have a very heavy diplomatic demarche to the allies that they should block it as well.

Thank you very much.

Chairman CRAPO. Thank you, Dr. Hufbauer.

Dr. Mulvenon.

STATEMENT OF JAMES MULVENON, PH.D., GENERAL MANAGER, SPECIAL PROGRAMS DIVISION, SOS INTERNATIONAL

Mr. MULVENON. Mr. Chairman, Ranking Member Brown, Members of the Committee, thank you for inviting me this morning. My name is James Mulvenon. I am the General Manager of SOS International's Special Programs Division. I spent the last 20 years building teams of Chinese linguist analysts supporting the intelligence community and Federal law enforcement and the Department of Defense primarily trying to understand Chinese technology trends.

Three years ago, with two of my U.S. Government colleagues, I wrote a book called "Chinese Industrial Espionage," which documented in tedious detail the extent to which the Chinese were stealing our technology which understandably made the Chinese government quite upset.

I would like to make four key points today. The first, I feel like my major role this morning is to present a more comprehensive view of the problem, as I see it.

China has a comprehensive strategy, in many ways unlike the U.S. Government, for national economic development and military modernization, which has unfortunately for U.S. companies created a very unfair asymmetric business environment in China for them to operate.

I have sympathy for the plight of U.S. companies in China. My father did business there for 25 years, but the nature of the environment that the Chinese government has created through regulation and other policies has in many ways forced U.S. companies,

which are in China and in the Chinese market for legitimate reasons, to grow and prosper and make money, to make suboptimal decisions, which may benefit that particular quarters numbers but may not be in the long-term interest of U.S. national security.

The second feature of the problem as I see it that U.S. laws have not evolved to really accommodate the creativity and innovation that the Chinese government and its entities are using in order to exploit the gaps and weaknesses in our system, moving as they found that they could not do straight acquisition through the front door through CFIUS, as they kept getting those rejected, but instead turned to more creative joint venture and investment vehicles to be able to back-door their way into intellectual property that they wanted to find.

And of this Chinese strategy, I think there are some key features: heavy state industrial planning like the "Made in China 2025" plan, military-civilian fusion, dispelling the notion that there actually is such a thing as a private company in China. The political and legal system in China really does not allow any company in China to be able to refuse the entreaties of the Chinese government if they wanted access to the technology—very heavy state subsidies, as was mentioned earlier. The integrated circuit fund of $250 billion was designed specifically to evade WTO prohibitions against state subsidies.

The promotion of national champion companies, we are all familiar with Huawei and its various activities. A whole raft of new laws and regulations that they have put out to codify what had previously been informal measures on their part, particularly the new cybersecurity law, which is putting tremendous pressure on U.S. companies for data localization, which is a threat to U.S. PII and other sensitive data.

Their creation of an entire domestic standards regime, they use as a trade weapon against U.S. companies. I would highlight 5G wireless standard is the latest iteration of that. A buy local strategy through their government procurement law, that puts pressure on U.S. companies. State-backed joint ventures and investment vehicles, which are quickly identified as state-backed. I would highlight Canyon Bridge, which is sort of a thinly disguised state council proxy of the Chinese government that attempted to buy Lattice Semiconductor.

The mercantilism that we see in the One Belt, One Road initiative, not to mention their planetary scale cyber espionage program that took all of our OPM data back to Beijing, large-scale technology espionage. Their nontraditional collection program, the so-called "1,000 Talents Programs," whereby they financially incentivize U.S. scientists and researchers to come back to China to be able to share that technology.

But in my view, export controls, which is often cited as the reason why we do not need FIRRMA, are not enough. I have many personal experiences with failing to convince Assistant U.S. Attorneys to be able to prosecute clear export control violation cases, but the anecdote that I would leave you with that is most troubling to me is the U.S. engineer who in its head possesses the kind of knowhow and information that would otherwise be subject to export control violations, sitting in a joint venture in China,

encouraged to help solve a particular technical problem. That conduit of information transfer is not covered under the U.S. export control regime, and it is why we need to more heavily scrutinize these overseas joint ventures and investment programs.

Thank you, sir.

Chairman CRAPO. Well, thank you very much, Dr. Mulvenon, and to all of our witnesses. Again, your testimony is fascinating, and you bring a wealth of knowledge to us. And we appreciate you doing that.

My first question is for Mr. Kupor and Mr. Mulvenon. The national security concern with venture capital arises from an assessment that China will soon surpass the United States as the technological leader in fields such as artificial intelligence and robotics in part derived from venture capital deals and special purpose vehicles, the latter formed to obscure the source of capital for a foreign acquisition.

My question is sort of a series of a couple of them. How do you assess the risk of early or growth stage venture capital contributing to the transfer of U.S. technology to the Chinese? And along with that, how is a venture capital deal different from a special purpose vehicle or a private equity deal?

Do you want to go first, Mr. Kupor?

Mr. KUPOR. Sure. Thank you, Mr. Chairman.

So, yes. First of all, with respect to China and artificial intelligence, there is no question—I think the witness talked about it—that China has very clear government policy around artificial intelligence. It was mentioned, and it is true, that they have offering things like cash stipends, for example, for U.S.-trained engineers who are Chinese nationals to come back to the country and obviously help them develop those technologies. So I do not think there is any question that there is a major technological race happening, particularly with respect to things like artificial intelligence.

On the venture capital side, the reason why, as I said, I do not think this is a major issue to worry about on the venture capital side is—number one is, at the end of the day from a U.S. venture capital perspective, the goal that we would like to see is how do we actually get foreign investment here into the United States so that the U.S. benefits from those technologies.

And as I mentioned, kind of as the global share of U.S. venture technology, venture capital has fallen, there are a lot more dollars competing for those deals from other geographies. So we think it is far better to actually encourage foreign investment into those companies.

On the venture capital side, specific to your question, what happens is venture capitalists are almost always minority investors in companies, and this is, I think, a very important distinction. You mentioned kind of private equity more broadly in buyouts. In buyouts, those tend to be controlled transactions, so those companies actually run the board. They control from an ownership perspective of the companies.

Venture capitalists are almost always minority investors, and so as a result, our ability to kind of dictate what the company does and to kind of share information from an IP perspective is much

more limited than it might be in an M&A or another control transaction.

So I think for that respect in particular, venture capital, in fact, is quite a very different investment category than you might be thinking about from some of the other investment categories.

Chairman CRAPO. Thank you.

Dr. Mulvenon?

Mr. MULVENON. Mr. Chairman, you mentioned earlier the DIUx report, which I associate myself with as well, and we collaborated with them in the creation of that report.

My organization also produced a study for the U.S. Economic and Security Review Commission on China's research into artificial intelligence and robotics and discovered—frankly were surprised by the extent of Chinese investment in early stage startups on both the West and East Coast of the United States, in that area, and our concern about it was, of course, derived from the Department of Defense's Third Offset Strategy, which explicitly calls out artificial intelligence and robotics and machine learning as the core technologies undergirding the next wave of U.S. military modernization.

And to the extent to which the Chinese government has a more robust investment strategy—and I think that has been carefully documented as to how much larger it is than the U.S. investment strategy—as well as the lack of scrutiny of these investments—and I would just highlight particularly in the DIUx category that there were certain investments, such as companies like Neurala and other places where there had been initial DoD funding, and because of the lack of nimbleness of our system, the Chinese then came in and did the second and third rounds of funding for those companies and then took over the seating of that research.

And so I think this is an area of great concern only because our own military leaders have identified these technologies as really what are going to be the game changers in the next round of military modernization globally, and given the amount of friction we currently have with the Chinese government in certain key security areas, if you have read books like "Ghost Fleet," which may be a hyperbolic view of the future, but are often seen by futurists as the role that things like artificial intelligence and machine learning will play, I think we need to look at this issue very carefully.

Chairman CRAPO. Well, thank you.

Mr. Padilla, the central point of your testimony is that FIRRMA broadens of the scope of CFIUS to something akin to a supra-export control agency with jurisdiction to capture outbound transactions, joint ventures, and other transactions outside the United States that are not investments and may even be licensed transactions that have consequences for critical technology companies and others.

What is the national security concern or gap in the export control regime or other enforcement mechanism that would necessitate this kind of expansion of CFIUS authority.

Mr. PADILLA. I think the concern that is driving some of what we are seeing in the debate about FIRRMA is that technology control lists need to be updated.

I would say that a couple of the technologies that Dr. Mulvenon mentioned—for example, artificial intelligence, machine learning, which IBM is very heavily involved in, things like quantum computing, Blockchain, these emerging technologies do not appear on the Militarily Critical Technologies List because DoD has not updated that list since 2011, nor have there been proposals put forward by the United States in the Wassenaar Arrangement, which is the international control regime that has existed really since the end of the Second World War through different names to try to control that technology on a multilateral basis to countries of concern.

So I think those are legitimate concerns, but I do not think the answer is to say, well, export controls are not working the way they were designed by Congress, so let us dump it all onto CFIUS. CFIUS is not equipped to do that kind of work. They are not equipped to look at new emerging technologies. They are not equipped to consult with allies. They are not equipped to impose multilateral or even unilateral controls.

So the export control system, which is under the jurisdiction of this Committee, I think needs a refresh, and I think the tools exist. They exist in regulation today, and they ought to be used. But I think simply throwing up our hands and saying, well, we would rather throw it all onto this other bureaucracy is not the right approach.

Remember it is the Committee on Foreign Investment in the United States. It was intended and created to look at inbound investment. If we do this, it would have to be renamed.

Chairman CRAPO. Thank you. I appreciate it. I have got to move on. My time has expired, and Senator Brown has——

Mr. PADILLA. Thank you.

Chairman CRAPO.——some really good questions, sir. But thank you for that.

Senator BROWN. Thank you, Mr. Chairman.

I was intrigued, Mr. Mulvenon, by your comment that there is no company in China that can resist entreaties to share—or turn over—may be a better term, technologies to the government, so thank you for that.

Dr. Hufbauer, good to see you again. Thank you for being here. You suggested some of China's trade practices may spur legitimate concerns, but that Congress should wait the outcome of the USTR study of the matter initiated last August.

I have great respect for Ambassador Lighthizer, but I am not sure we can or should wait for another study. I would like to ask you and then each of the panelists. Is there any doubt that China has and continues to violate its international trade commitments and that engages in unlawful technology transfers?

Start with you, Dr. Hufbauer.

Mr. HUFBAUER. No doubt whatsoever.

Senator BROWN. Mr. Padilla?

Mr. PADILLA. I would agree. I do not think there is much doubt of violations, including by companies like ZTE most recently.

Senator BROWN. Mr. Kupor.

Mr. KUPOR. I am definitely not an expert on the topic, but certainly, from my understanding, that is true. Yes, sir.

Senator BROWN. Mr. Mulvenon.

Mr. MULVENON. I think it is not only true, but I think every day, we uncover more and more of the scope and scale of it and never cease to be amazed by the size of the transfer.

Senator BROWN. OK. Thank you.

Mr. Padilla, I agree that we should be careful not to ask too much from CFIUS, as your testimony pointed out, but when it comes to national security, do we need to choose between export controls, which you admit are outdated in CFIUS, and why not adopt an appropriate that tries to fill the gaps between the two?

Mr. PADILLA. Well, CFIUS reviews do look at export controls. When I was Assistant Secretary of Commerce, I sat on the CFIUS committee, and one of the things we looked at when we were looking at an acquirer, for example, is do they have a history of violating export control laws. Could the acquirer be trusted to follow our laws, or were there concerns there? So I think there is close interlock between the systems, but they were built very differently, and they have evolved very differently over the course of 70 years in the case of the export control system to do different things.

And I think the answer is to improve the export control system, also to improve CFIUS because there are some gaps in what it can look at, but not to layer them on both together, so that the same transaction that might not need an export license or that might have received one also then has to go through a redundant CFIUS review. I do not think that is an appropriate approach. I do not think it would enhance security, and it certainly would hurt competitiveness.

Senator BROWN. Thank you.

Mr. Mulvenon, there is broad agreement, I think, that the identification of technology that should not be transferred to our adversaries lags well behind where it should be. Will it not be a problem that wherever you locate the responsibility, DoD or CFIUS or Commerce? So why is CFIUS in your mind the best place to place that responsibility?

Mr. MULVENON. First of all, I agree with Mr. Padilla about the laggard updating of the MCTL, which is really the most powerful resource we have for tracking these kinds of technology developments, and many, many times in my own professional experience, I ran into situations in which we could not convince key decisionmakers about an export control violation because of the delay in adding new technologies to that list.

I would highlight, however, that in terms of the gaps between the systems, I could give you a good example of where the two systems are not interacting well terribly.

The Commerce Department denied entity export list has not been updated, for instance, to reflect certain recent CFIUS actions. There is a Chinese company called San'an Optoelectronics, which is a chip firm that has twice been blocked by CFIUS from attempting to acquire military sensitive technology, which is not on the denied entities list, and American firms continue selling sensitive technology to them and discussing investment in those companies. And so that is a good example where the two systems need to interact better because I certainly see them as complementary.

I do not see FIRRMA as a threat to become a supra-export control agency. I see us needing to fill the gaps on both sides, of both

the export control system as the first line of defense, and then CFIUS as a second line of defense, particularly related to investment and joint ventures.

Senator BROWN. So talk just for a moment in the last minute or so about developing these lists. It seems that as we move from 200 CFIUS filings a year to perhaps many, many more than that, how do you organize these lists across so many agencies?

Clearly, there will be case-by-case determinations, but they obviously need more structure than that. How do we do that better?

Mr. MULVENON. Well, I mean, the suggestion earlier about the National Academy of Sciences and other entities that are actually more directly interfacing with the cutting-edge technology, that is always the dilemma when I deal with elements of the U.S. Government is that they are not always on the cutting edge of understanding which technologies are emerging at any particular time. And so I think there are those kinds of outside partnerships whereby you can maintain, then be current about the technologies we should care about rather than putting an undue burden on U.S. Government agencies that really do not have the kind of day-to-day expertise to be able to track that.

Senator BROWN. [Presiding.] Senator Toomey.

Senator TOOMEY. Thanks very much. Gentlemen, I appreciate the testimony today. I am very sympathetic with the goals of this legislation, but I do have some concern about unintended consequences.

My concern arises from a starting point that foreign direct investment is a huge and hugely important engine for growth in the United States.

The tax reform we just completed, I think is going to encourage significant increases in foreign direct investment because we are going to lower the burden, the tax burn on the returns on those investments. I think this is a huge driver of growth, and yet there are legitimate concerns about whether there is some security that—security issues.

So I just want to figure out how we strike the right balance here. One of the concerns—and maybe Mr. Hufbauer could address this—is so much of the kind of technology that we would be worried about transferring is inherently mobile. It can be developed and refined and improved almost anywhere in the world. If we do not strike the right balance here, what is the risk? And maybe under this legislation, would you be concerned about really constructive innovators being driven overseas because they are concerned that if they are domiciled in the United States, potential future investment is too limited? Is that a concern?

Mr. HUFBAUER. Thank you, Senator. Yes, that is very much a concern, and the way I would put it is this—U.S.—well, during my lifetime, which dates to before the Second World War, the U.S. Government has been a leading proponent of technology, DARPA and ARPA and so forth, and of course, companies. It is that investment at home that has given us this leadership, and our big weakness is not the espionage by the Chinese or their forced technology transfer. Our big weakness is that we may not be keeping up the pace of investment in innovation that we had.

At one time, we were clearly the leader. You cannot really say that so strongly today, and the leadership has a couple of components. One of the components is making the United States a very attractive place for foreign scientists and engineers and so forth to not only get their degrees here but to stay here.

Senator TOOMEY. So in its current form, are you concerned that this legislation could tend to have that effect of driving some innovation overseas?

Mr. HUFBAUER. Well, I think it is flexible enough that it would not necessarily have that, but I do not want to see the U.S. Government put all its emphasis on trying to build a wall on the outward flow of technology.

Senator TOOMEY. Well, that is another concern. That is another——

Mr. HUFBAUER. That will never work. I mean, we have to do more at home, and that is by far, the bigger part of the story.

Senator TOOMEY. I have only got 2 minutes left. Let me put another issue out on the table and invite anyone to comment on either my first question or this next one.

The next one is—let us be honest. Incumbent businesses are never enthusiastic about a dynamic innovative competitor emerging, and I worry that large powerful incumbent businesses might attempt to use CFIUS as a way to protect their status and diminish the opportunity of potential competitors to raise the capital that would allow them to compete.

Do you believe that there are sufficient safeguards in this legislation to minimize the risk of that unintended adverse consequence?

Mr. PADILLA. Senator, I will maybe take the first stab. When I served in Government, I saw cases like what you just described, where it was clear that an incumbent competitor was trying to prevent a foreign investor who would then infuse capital into a relatively weaker domestic competitor and strengthen themselves in the process, and we tried very hard in the Bush administration at least not to allow that dynamic to take hold because it is improper.

On your first question, I would just comment. IBM has 12 research laboratories around the world. Most of our cutting edge research on things like AI and quantum computing are done in New York or Texas or California, but we also have labs in places like Zurich, Switzerland, and Sao Paulo, Brazil.

And I can tell you that if FIRRMA goes in the way that it is written now, there would be large incentives to move core research outside the United States, so that it would not be captured by some of this added bureaucracy, and that is not a good thing. It is not what IBM wants to do.

Mr. KUPOR. Senator, if I could just add to your first comment as well, your first question, there is no question that kind of engineering talent will follow capital, and we have got case studies of that already today in the form of Government incentives that are driving capital. So whether that is R&D tax credits, for example, that Canada and France and others are offering to engineers—it was mentioned that China obviously is trying to attract a lot of its expat community back through financial incentives.

So I think it is a microcosm of a broader problem that could be here, which is if you stifled capital flows, you could have talent flow out as well.

Senator TOOMEY. Thank you very much.

Ms. DOWNEY. Senator Schatz.

Senator SCHATZ. Thank you, Ranking Member Brown.

Mr. Padilla, I have a question, just a practical question about the capacity at CFIUS. How many employees does it have? How many analysts? What is the funding level? Because as we consider expanding its scope, it is going to matter whether or not they can accomplish anything additional.

Mr. PADILLA. I do not know the exact current number, Senator. It has been a little time, about a decade, since I was involved, but when I was there, there were less than 20 full-time staff at the Treasury who were focused on this, and then you had in each agency—I was at the Commerce Department. We had three people under me at the Bureau of Industry and Security who worked on this.

So I would guess the entire universe among all the agencies, maybe about less than 100.

Senator SCHATZ. OK. So if you are talking about fewer than 100 people, one of the questions is—it is an appropriations question. It is a resource question. It is a throughput and capacity question. Setting aside whatever statute CFIUS hangs its hat on, we could give them more things to do, and if it is the same number of people, they are not going to be able to accomplish it.

I have a question about early stage investment and potential dual use, and it seems to me this is an appropriate thing for CFIUS to look at, but it is a little dicey in the sense that you have a startup company, and they are not sure at the outset—I mean, technology has evolved, and their application has evolved. So a company may not know that it is going to be dual use until the research finds a defense application.

So at what point does CFIUS—I mean, how do you strike that balance between sort of not snuffing out anything that could potentially be dual use in the future, which would pretty much snuff out 90 percent of tech startups, but recognizing that once something has a serious defense implication and application, that then it is under CFIUS jurisdiction. But how do you sort of—I am looking at the two of you here—strike that right balance between CFIUS and the VC and startup community?

And I will start with Mr. Padilla and then go to Mr. Kupor.

Mr. PADILLA. It is a very hard balance to strike, Senator. I do think—and I support the idea—that CFIUS does need the authority to at least look at nonpassive, noncontrolling investments. In other words, it is not just passive, but it may not constitute control.

You could look at things where someone gets a board seat on a company. It is not a controlling interest, but because they are on the board, they have access to information that they might not otherwise get. And I think it is appropriate that CFIUS be able to at least inquire about that.

In terms of what technologies, here again, I think it is incumbent on the Government to define what it is worried about. That is why Congress created the Militarily Critical Technologies List, and it

cannot just be we are worried about AI. It has to be more specific than that, and that is hard to do. I used to do it. It is not easy to say this parameter or this algorithm.

But if the Government is concerned about security, it is incumbent on the regulator to define what it is regulating. I do not think the right approach is to say bring us everything in a very broad universe, and we will sort it out one by one and tell you later what we are worried about. That is not a good regulatory approach.

Senator SCHATZ. Mr. Kupor.

Mr. KUPOR. Yeah, I agree with that, Senator.

I think also you are right, which is as startup companies develop, of course, the products go through many iterations. So I think it would be very hard for CFIUS to have any ability to review kind of the criticality of that technology until there is a true commercial application developed that actually has dual use, and that is going to often come probably 3, 5 years into a company's history. So at that point in time, many of its investment dollars will have actually already been received by the company. So you may be talking about retrospectively trying to undo financing agreements and other stuff that has happened. I think it is a really hard problem to handle. I wish I had a more definitive answer for you, but I think for that reason, it is very difficult to kind of think about cutting off that early supply of capital before you actually understand what the commercial use of that technology is.

Senator SCHATZ. So I have maybe a tougher question for the whole panel, and it has to do with CFIUS was constructed to be limited in scope because of how serious the matter is because to have the Government intervene against a transaction is no joke, to expand that, and yet it still has to have confidentiality because a lot of the discussion is a national security discussion. There is a logic to that on the other hand. Then you have a black box with, say, 100 human beings, and maybe even few are making determinations on which companies get investments and which do not, and maybe only in the SCIF can Congress exercise its oversight. And that seems scary from the standpoint of the potential for crony capitalism, of the potential for corruption. And I am wondering whether you can just speak to that very briefly as my time expires.

Mr. Padilla, and then quickly all the way down the line.

Mr. PADILLA. CFIUS is one of the least transparent Government processes that deals with foreign commerce. The export control system for whatever faults it may have is relatively transparent. The business community knows how to do it, knows how to work with it. CFIUS by contrast is very opaque.

Mr. KUPOR. Yeah, I would agree. I think if this institution decides to go forward with legislation, I think—deferring too much of the rulemaking authority of CFIUS is a real problem, just given kind of the confidential nature of it. So I think having very clear bright-line rules about what is covered and what is not, it would be incumbent upon this organization to do so.

Mr. HUFBAUER. That is a very legitimate concern, and my suggestion is that the Congress ought to on a secret basis take a report from the CFIUS maybe every year, every 6 months, and review the cases which were blocked or the cases which were maybe not formally blocked but turned back and get your own judgment,

because it is obvious that CNI and the CIA and the Pentagon and so forth who have all the secret information, which we do not want to disclose widely to the public, but Congress should take a look.

Mr. MULVENON. Senator, I think one of the tradeoffs that is important, particularly when I talk to companies about their frustration with the process is that there could be—and there is some language in the bill right now that suggests this. There could be a greater opportunity for the companies earlier in the process to provide their own technical assessments of the technology issues at play as well as a commitment to resolve the CFIUS evaluation at the first level much sooner as a tradeoff to incentivize companies for the fact that they are expanding the scope of what is being reviewed. And I know that was tremendously frustrating to Western Digital and others that were involved in the process, how long it took.

Senator SCHATZ. Thank you.

Chairman CRAPO. Senator Menendez.

Senator MENENDEZ. Thank you, Mr. Chairman.

So let me first take a point of personal privilege and say, Mr. Kupor, you have a great guy working for you in Justin Field. He was my finance guy. He is in the audience, and my mom said if you can say something nice, say it; if not, keep quiet. I can say something nice. He is a great guy.

Mr. KUPOR. Thank you, Mr. Senator. I agree with you.

Senator MENENDEZ. And I also see that another alumni of my staff, who was my communications director, Matt Miller, is back there, sitting back there. I do not know who you are representing here today, but, Matt, it is good to see you.

I thank all of you for your testimony. Dr. Mulvenon, a draft report prepared for DoD last year raised concerns about certain activities by Chinese firms in the United States that appear to be motivated by transferring innovative technologies to China with the ultimate goal of giving China a competitive advantage and specifically to report highlights to Chinese venture capital investment in early stage startup firms in the United States in the artificial intelligence robotics financial technology sectors.

It raises concerns that these investment activities are both part of a larger Chinese strategy to displace U.S. businesses and certain industries and are specifically structured to fly under the radar of the CFIUS review process.

In your testimony, you discuss how China has structured certain technology investments in the United States to essentially get around the CFIUS reviews. What are the vehicles or investment structures that they are using to do this? And in your opinion, what steps should the Committee consider to ensure that those types of efforts are actively monitored, tracked, reviewed, and then appropriately done so by CFIUS?

Mr. MULVENON. Thank you, Senator.

Well, in fact, if you look at artificial intelligence, you can go all the way down my structure of China's comprehensive strategy and pick off the pieces of each one.

China has a national industrial planning strategy for artificial intelligence development, including the corresponding military artificial intelligence development. They have a massive subsidy

system set up, just structured in a way that evades the current WTO restrictions on state subsidies. They have identified national champion companies within China that they want to be leaders on artificial intelligence. They have designed laws and regulations that insist on data localization, such that those artificial intelligence efforts, that that critical intellectual property data has to be stored in China if that work is going to be done there.

They have a domestics standards regime that they are using as a trade weapon in order to leverage using market access in China to leverage technology transfer for multinationals, and then they have state-backed investment vehicles focused on artificial intelligence investments.

Senator MENENDEZ. So how do we respond to that?

Mr. MULVENON. Well, first of all, recognizing that it is a comprehensive strategy rather than the individual actions of self-interested financial actors, which was our first cut at the problem, and recognizing, as Dr. Hufbauer would say, there is unfortunately on our side a realization that we are not investing enough. So let me always say that we need to do more investment on our side in artificial intelligence rather than simply block Chinese efforts to invest in artificial intelligence in the United States, and we are woefully inadequate on that front.

But also just clearly recognizing in many cases the thinly disguised state and military origins of many of these investment vehicles from the Chinese side and scrutinizing those and not permitting those to harvest the best of the emerging technologies in the United States.

Senator MENENDEZ. Thank you.

Let me ask you this. The legislation being discussed today includes a provision that would make mandatory CFIUS filings for transactions that involve certain investments by state-owned enterprises. This has been an issue of mine going back to the Dubai Ports World deal in which CFIUS approved a transaction that would have handled over control the port operations in New Jersey, New York, Baltimore, and Miami to a state-owned company in the United Arab Emirates.

In September, the Committee heard testimony from the former Treasury Assistant Secretary, Clay Lowery, who oversaw CFIUS. He told the Committee that it was a worthwhile exercise to explore the idea of mandatory filings for state-owned companies as opposed to the current regime of high scrutiny for those transactions.

What are your views of a mandatory filing requirement for transactions involving investments in the United States by state-owned or controlled enterprises?

Mr. MULVENON. Well, with the caveat, as I said earlier, that under the current Chinese political and legal system, principally given Chairman Xi Jinping's assertion that there needs to be greater Communist Party penetration even into private enterprises in China, there is an element of it that is a false distinction, given the Chinese government's ability to reach into private companies and get access to technologies, but I do believe that state-owned enterprises should be mandatorily reviewed, if only because when we have peeled back various investment efforts in the last couple of years and found them to be actually state-backed and state-owned

enterprise-backed investments, that those were—that was the primary basis of the security concern.

And given the nature of the Chinese system of state capitalism, I think those state-owned enterprises deserve particular scrutiny.

Senator MENENDEZ. Any other views on that? And then I will close on that.

Mr. HUFBAUER. I agree, totally.

Mr. PADILLA. I would agree also, Senator. I worked with Clay Lowery when he was at Treasury and I was at Commerce, and the FINSA bill, the last bill Congress passed on this, did increase the scrutiny, and perhaps another increase of scrutiny would be appropriate.

Senator MENENDEZ. Thank you.

Senator BROWN. Senator Warren.

Senator WARREN. Thank you, Mr. Chairman, and thank you to our witnesses for being here today.

The Committee on Foreign Investment in the United States, CFIUS, that we have been talking about reviews acquisitions by foreign companies to ensure that they do not threaten our national security, and at our last hearing, we discussed how technology transfers from our companies to foreign competitors can undermine our security and how CFIUS does not cover certain transactions where our adversaries are intentionally investing in American startups in order to get access to critical testimonies.

But I want to ask a different question around this. When CFIUS does review a transaction, it can approve it with a mitigation agreement that requires companies to complete certain steps in order to reduce the national security risk.

Now, CFIUS is supposed to ensure that parties implement the mitigation agreement, but a draft Pentagon report issued in February of 2017—I think Senator Menendez just referred to it—advised that CFIUS should try to minimize reliance on these agreements because they are difficult to enforce, and there are not enough resources decided to monitoring them.

So, Dr. Hufbauer, are more investigations into the national security risks of transactions become necessary, how can CFIUS ensure that a mitigation agreement is maintained over time if overseeing that agreement may be too costly or addressing security risks if the transaction may be too complicated?

Mr. HUFBAUER. Thank you, Senator.

It is a problem because as Chris Padilla said, there is only about 100 people on the staff of CFIUS, and it is hard with that size staff to do all the follow-up that is necessary.

So if this bill becomes law, there has to be a substantial expansion, but in addition, I would suggest that where there is a mitigation agreement, which obviously the company wants, the acquiring company and probably the acquired company, they should put money into some kind of escrow in the Treasury to ensure the enforcement over a period of years, 5 years, 10 years, to take care of the financial burden that this will entail.

Senator WARREN. Interesting idea. Thank you.

I should note that the defense authorization bill that passed Congress last year requires a multiagency report that includes an assessment of whether current CFIUS process provides adequate

monitoring and compliance, and I think we need to work through this and need more good ideas on how to do this.

The discussion of CFIUS focuses on protecting our national security while preserving foreign investment, but I want to touch on a policy that I think protects both priorities, and that is investment in basic research.

Jim Lewis, a former official with the Departments of State and Commerce, testified in this Committee last year that CFIUS reform should be paired with policies that drive innovation right here at home, and that means investing in research that helps our economy and our military.

He said that our underinvestment in scientific research, quote, creates a self-imposed disadvantage in military and economic competition with China, and that maintaining our economic and military superiority requires investment, both by encouraging private sector investment and by Government spending in those areas like basic research where private sector spending is likely to be insufficient.

So let me start with you, Dr. Hufbauer, again. Would more Government investment in scientific research support the core objectives of CFIUS by protecting strategic industries from foreign competition and maintaining our technological advantage?

Mr. HUFBAUER. Yes. When you were out of the room, Senator, I gave a big plug for more investment, both by the Government and by private firms.

Senator WARREN. I want to give you as many chances as possible.

Mr. HUFBAUER. Well, in any event, yes, this is the big picture. What we do to stir innovation in this country is substantially more important than what we do to block outward technology going to China or Russia or these countries, and we should do more. We are not very good right now.

Senator WARREN. That is very well stated.

Anyone else like to weigh in on that?

Mr. KUPOR. I would just like to underscore that doubly. Yeah, I think that is exactly right. There is no question that what we are up against, our foreign governments, who have very kind of centralized groups that they put together from a funding perspective, to attract talent, to build technologies—and there is a lot more we can do in the United States, no question.

Senator WARREN. Anyone else want to add or just say yes, yes, so I can get a good record here?

Mr. PADILLA. I would strongly echo the comments of my colleagues, Senator Warren.

Senator WARREN. Good.

Mr. MULVENON. I strongly agree with you, Senator, particularly given the, frankly, staggering scale of the investment that the Chinese government is putting into advanced technologies right now.

Senator WARREN. Well, I really appreciate it, and thank you all on this.

I think it is important to stand up to unfair commercial practices that harm our economy and threaten our national security, but I also think we need to make the necessary investments here at

home in our own research. That is what keeps us strong, and that is what gives us a true advantage.

So thank you.

Thank you, Mr. Chairman.

Chairman CRAPO. [Presiding.] Thank you.

Senator SCOTT. Thank you, Chairman, and I want to say thank you to Senator Cornyn for being here this morning and his testimony and his continued efforts on this very important issue.

South Carolina is the home of a number of incredible companies. We are one of the largest beneficiaries of foreign direct investment. There are 1,200 foreign-owned entities that have created or are currently employing 130,000 South Carolinians. Two-thousand fifteen alone saw $2.4 billion of foreign investment in South Carolina. 2011, a few years earlier, was the height, the peak at $3.7 billion of FDI.

Whether it is Bridgestone in Aiken, Honda in Florence, Mercedes in North Charleston, foreign companies are flocking to South Carolina, and this is not an ad for South Carolina, but who can blame them? We have world-class universities, a world-class skilled workforce, and an incredibly high quality of life. From the beaches of the low country to the mountains in upstate, South Carolina has something to offer for everybody.

Our state would not be where it is, however, without foreign investment. That said, it is clear to me that some are taking advantage of our system of trade to the detriment of our Nation's security.

Last year, I joined with Senator Cornyn in introducing the Foreign Investment Risk Review Modernization Act. The bill expands the committee's jurisdiction to include real estate purchases around military basis in light of the documented attempts by the Chinese to spy on our armed forces.

We also updated the committee's definition of critical technologies, just as a development of AI and advanced genetic engineering is taking on.

So, Mr. Mulvenon, why is it so important for CFIUS to review these kinds of transactions and specifically those transactions around military bases that seem to be—land transactions around military bases that seems to be a sore spot as it relates to the Chinese trying to take advantage of opportunities to spy on our armed forces?

Mr. MULVENON. Well, Senator, it is an excellent question. If you look at this raft of new laws that the Chinese have put out, one of the most striking parts of it is their view of extraterritoriality with respect to Chinese companies.

And the extent to which the Chinese military and their security services can directly intervene in the operations of these companies to benefit Chinese national security, as an example, if a Chinese telecommunications company is operating a network operations center in the United States, according to their new national security law, state security personnel can enter that facility in Plano, Texas, for instance, and do lawful intercept of communications in that facility because they are treating that Chinese company as a domestic Chinese company rather than one operating on foreign soil.

That is why the decision to reject the purchase of that wind farm in the Pacific Northwest is particularly relevant because those facilities in that wind farm would have been able to collect emissions from a Navy electronic warfare facility that was just there on shore. And those emanations would have been able to reach those wind farm turbines.

And so I think that that is the particular concern, that the ability of the Chinese government to impose upon these companies involved in the Chinese side of the transaction and to use those corporate facilities as intelligence collection platforms.

Senator SCOTT. Thank you.

Would you say that we have done our best to strike a proper balance between our economic concerns and our national security concerns within the bill? Do you think we have hit that sweet spot?

Mr. MULVENON. I do think there is a good balance in the bill. I favor the bill because I believe it responds to very creative Chinese attempts to exploit gaps and weaknesses in our current system.

I do not believe that the bill is a death knell for innovation or investment in the United States, but I believe that given the scale of Chinese technology espionage of the last 15 to 20 years, most of which has gone unchecked, that frankly we need to swing the pendulum a bit more in the other direction.

Senator SCOTT. Thank you.

With my remaining time, Mr. Padilla, I am appreciative of IBM's growing presence in South Carolina as well. I read your letter expressing concerns regarding our efforts to reform CFIUS. Your claim that FIRRMA would subject hundreds of transactions unrelated to national security to a committee review, I want to hear you out and get your perspective as we share the goal of protecting our country. What specific changes do you envision for us to improve FIRRMA and to meet the mutually important goals?

Mr. PADILLA. Thank you, Senator, and South Carolina is a great place to do business.

Senator SCOTT. Yes, sir.

Mr. PADILLA. So thank you for your support.

My concern with the bill boils down basically to one section, and it is Section—it is in the definitions, Section B, Roman Numeral V, and it is the provision that would do what I have described as problematic. It would expand CFIUS from looking at inbound investment to looking at outbound transactions. And it has the language that I referred to in my testimony about the contribution of any technology or IP through any form whatsoever.

I think if you change that provision and a couple of other definitions, much of what the rest of the bill does, IBM would support, including, by the way, expanding the jurisdiction of CFIUS to look at real estate transactions. That is one of the gaps that I identified that does need to be filled and needs to be filled by legislation.

Senator SCOTT. Yes, sir. Thank you so much.

Thank you, Mr. Chairman.

Chairman CRAPO. Thank you.

Senator Van Hollen.

Senator VAN HOLLEN. Thank you, Mr. Chairman, and thank you to the witnesses.

Before I ask the witnesses a question, I just wanted to address a question to you and the Ranking Member regarding another issue of national security, which is the North Korea situation. Under your bipartisan leadership, Mr. Chairman and Ranking Member, this Committee unanimously passed legislation, I think important legislation, to strengthen and better enforce sanctions against North Korea.

We passed that unanimously out of Committee on November 7th. Since that time, on November 29th, North Korea tested another ICBM missile, and just 2 days ago, despite the environment with respect to the Olympics and some of the talks that are taking place, Secretary Tillerson said that "the threat is growing" because even as those talks take place, the North Koreans continue with their program.

So my question, Mr. Chairman, could you give us an update on the status of this legislation which passed unanimously out of this Committee? I just want some assurances that we are going to get a vote on this as soon as possible in the full Senate.

Chairman CRAPO. Yes, Senator Van Hollen. I will be glad to give you my update and then also turn to Senator Brown for his response as well.

I remain solidly committed to moving this legislation not only on the Senate floor as quickly as we possibly can but also encouraging prompt house action, so that we can get the bill to the President's desk. We do need to stand firmly and strongly with regard to the developments in North Korea, and I believe the legislation that you have helped to draft and bring forward is a very critical and important part of that.

As you know, we have been running into some difficulty getting the necessary consents from the other Senators to move on the floor at this point in time. I am continuing to work with all of the Senators to get those roadblocks removed.

As is often the case, the roadblocks do not necessarily relate to this legislation, but the politic of the body result in us having to resolve some other issues as well, which we are working on as recently as yesterday. We have had meetings on trying to move it.

Although I cannot tell you yet that we have got everything ironed out in terms of the process to move forward, I can reassure you that I am committed firmly to doing it.

Senator VAN HOLLEN. Thank you, and I appreciate that, Mr. Chairman.

Senator BROWN. Thank you, Senator Hollen. I concur with the Chair and strongly support this bill and this vehicle and moving on the floor as quickly as we can, understanding the roadblocks that have been thrown in front of us.

I spoke briefly at the White House last week with Secretary Tillerson. This is important for a whole lot of reasons, as you know, and we will work together to remove those roadblocks and work with you. And thanks for the work. You have really kept this going and kept this in front of us and in front of the public, so thank you.

Senator VAN HOLLEN. Well, thank both of you, and Senator Toomey was here earlier. He said he would join me in full support of the effort, and thank you both of your effort.

Chairman CRAPO. Thank you.

Senator VAN HOLLEN. I just think we need to move it as quickly as possible because I do not know of any real substantive on the merits objection, so thank you.

Chairman CRAPO. You are right. Thank you.

Senator VAN HOLLEN. And I do not have a lot of time left, but I do want to ask Mr. Padilla. You mentioned in your testimony when I was here earlier your concerns about essentially using CFIUS for U.S. exports as opposed to investments here in the United States, but you said with respect to investments here in the United States, you thought we could strengthen the current regime.

What are some specific ideas? I am trying to look for some common ground here. We can figure out what we disagree on and what we agree on.

Mr. PADILLA. Sure.

Senator VAN HOLLEN. What is it that specifically we can change with respect to CFIUS?

Mr. PADILLA. Well, one is the one that Senator Scott mentioned, the ability of CFIUS to look at real estate transactions that are in close proximity to Government or military installations.

The second would be what I would call nonpassive but noncontrolling investments. Right now, CFIUS looks at—if you control an acquisition, it is not worried about passive investment, but what about that gray area in between, where, say, you get a board seat on a company, and you get access to certain controlled information, but you may not "control" the company. That, I think is an area for expansion.

The other would be more process-related, and that is, I think there should be a senior Senate-confirmed official in every CFIUS agency who signs off on the transactions. I did that when I was at Commerce. I know some agencies do it. Others do not. And you need that senior-level review. Dubai Ports World showed that when you do not have that, you can have problems.

Senator VAN HOLLEN. Got it. Appreciate that.

The one area that we would not be able to address, the issue that Dr. Mulvenon raised earlier with respect to the kind of joint venture in China, where it amounted to a directed Chinese effort to gather more important information in some of these very innovative areas.

So we are going to have to bridge your proposals where there was agreement on the U.S.-based investments with some kind of——

Mr. PADILLA. I think you can do that, Senator, through enhanced export controls, and there is already authority to do that. It is not being used to its full potential.

Senator VAN HOLLEN. Dr. Mulvenon, would enhanced export controls be enough? Because I heard your earlier testimony. I think that was important that we have not—since 2011, I think you said—updated that.

Mr. MULVENON. My concern—I can give you a scenario, a very simple one that is my main concern. A lot of export control cases and the technology control and mitigation plans that I have seen developed dealing with that, where you de-architect, where you defeature a technology to take out the 30 percent of that technology

that is covered under the export control regime, the technology is then transferred.

But then in the context of the joint venture, the engineers potentially who have that additional—that remaining 30 percent of the knowhow in their heads and then they are working on common problems within the joint venture and everyone is committed to making the joint venture a success, my concern is the export control system does not cover the bleed of that potential last 30 percent to re-architect it back into the technology after the export control system successfully had to de-architect it. And that is the dilemma about joint ventures and investment vehicles particularly located in China.

Senator VAN HOLLEN. Let me just correct a factual point. The export control system actually does control that transfer of knowledge. There are deemed export laws on the books that say if you have something in your head and you are subject to U.S. jurisdiction, you cannot tell anybody about it without a license.

Now, there may be issues about whether it is being followed or not, but that is an enforcement problem, not a legal jurisdiction problem.

Mr. MULVENON. My only point, Senator, is that, of course, it falls under deemed exports, and we have a whole variety of deemed export problems, not the least of which is PRC nationals at U.S. universities operating equipment in laboratories that would have required a deemed export license if they were using them at a facility in China, but they are allowed to use them at a university in the United States in a hard science program. So there is a whole range of problems we have on the deemed export side, but the problem is the enforcement regime, a commercial enterprise in China of that last 30 percent, that there is no good mechanism for the enforcement other than the good will of the people involved in the enterprise.

Senator VAN HOLLEN. Thank you. Thank you both.

Chairman CRAPO. Senator Jones.

Senator JONES. Thank you, Mr. Chairman, and I apologize for being late. Thanks to all the witnesses for being here. I have got just a basic—not in the weeds, but just kind of simple questions.

I know, Mr. Kupor, you expressed some concern about a bill that might chill foreign investment, and it is my understanding that to date, there have been four transactions blocked by presidents as a result of the CFIUS review. Do you have any information of other potential deals or investments that might have been either withdrawn or otherwise scuttled because of the possibility of CFIUS review?

Mr. KUPOR. No, not specific to the venture capital world.

What my specific concern was, if we sweep up foreign investment in two areas—one is as limited partners in U.S. venture funds, then that would obviously chill the ability for non-U.S. investors to be able to participate and help us grow those technologies.

And then the second specific question was if you have foreign direct investment into a venture capital company, a little bit to the point that was made to Mr. Padilla about kind of nonpassive investments, making sure that we are very clear about what the rules of the road there are, so that we understand at the outset,

if we are going to take money from a foreign investor, what are the things that we need to ensure so that information disclosure is appropriate and consistent with U.S. law.

Senator JONES. OK. And does this bill address concerns about foreign investment, or can we make it better?

Mr. KUPOR. The broader objectives of the bill, we are very comfortable with. Again, it is these specific areas where our concern is there is enough vagueness in the way it is written that it could chill this investment, and so our request would be for this institution to make sure that we define those more appropriately as part of the legislation process.

Senator JONES. OK. Very good.

What about green field deals, the ones that U.S. businesses—you know, that did not exist prior to the investment by foreign person or entity that seemed to be beyond the reach of CFIUS? Is that covered by any other rule, regulation, or something that is out there, or should we covered green field, the new deals that come in that are beyond CFIUS control right now?

Mr. KUPOR. Just so I am clear, Senator, do you mean new deals as in kind of startup companies?

Senator JONES. Yeah. That did not exist prior to the foreign investment coming in, that is part of a new deal.

Mr. KUPOR. I think it is very reasonable that to the extent a U.S. company, a new startup is going to take money from a foreign investor, I think it is very reasonable for us to have a defined process to understand does CFIUS apply, and if so, are there things that the U.S. company can do to make sure that they are compliant with it, whether that be board seats, whether that be information disclosure, those types of things.

Right now, at least our concerns, it is not well defined there, and so what a passive investor actually is, is a largely undefined term of the bill.

Senator JONES. All right.

Mr. Chairman, that is all I think I have. I am going to resist the urge to go toe-to-toe with Senator Scott about Alabama versus South Carolina, especially in light of the most recent football games.

[Laughter.]

Chairman CRAPO. Well, thank you very much, Senator Jones. Those are the kind of fun little battles that you can have on the sidelines, anyway.

That concludes our questioning, and again, I want to thank our witnesses. You all have a wealth of knowledge. It is very obvious, and we have some very tricky and complicated issues to resolve here and roads to travel on this. But we must get it right, and we must do it well.

And so I am sure that we will be in continued contact with you. As a matter of fact, it is a practice for Senators who did not get all the time they wanted or who did not have an opportunity to send some questions to you after the hearing. I would let those Senators know that those questions will be due by Thursday, January 25th, and then ask each of you, if you get additional questions following the hearing, if you would respond to them as quickly as you can.

Again, we appreciate your being here with us today and your attention to not only this legislation and the issues we are grappling with right now, but the overall set of issues of protecting our U.S. national security on these critical technologies.

And with that, this hearing is adjourned.

[Whereupon, at 11:18 a.m., the hearing was adjourned.]

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

PREPARED STATEMENT OF CHAIRMAN MIKE CRAPO

JANUARY 18, 2018

Today the Committee will begin to evaluate the essential national security elements underlying a comprehensive proposal to reform the review process used by the Committee on Foreign Investment in the United States, or 'CFIUS.'

Thank you to Senators Feinstein and Cornyn for their testimony on their bipartisan Foreign Investment Risk Review Modernization Act of 2017.

This bill was first introduced by Senators Cornyn and Feinstein on November 8th to 'modernize and strengthen CFIUS to more effectively guard against the risk to the national security of the United States posed by certain types of foreign investment.'

The Senators and their staff have worked over a year with concerned national security officials, the Treasury Department and various affected industry representatives.

This comprehensive bill could be the first update to the body of CFIUS law in more than a decade. It would expand the reach of current law in a number of respects, while codifying some current administrative practices, and result in significant changes to jurisdiction, process and enforcement.

A study produced for the Pentagon's DIUx unit, which enlists startups to find solutions for the military's most advanced technology-related requirements, is credited as being the catalyst for much of the impetus behind this CFIUS reform.

The DIUx study highlights the problems arising from the fact that the U.S. Government does not currently monitor or restrict venture investing, nor stop potential transfers of what's known variously as early stage, foundational or critical technology know-how, particularly with regard to certain types of Chinese investment in the United States.

Today's hearing also draws witnesses from one perspective of the private sector that is concerned not only with inbound investment, but also outbound transactions and from the venture capitalists that support American innovation.

We are also joined by two long-time CFIUS analysts, with particular expertise in regard to China's economy, trade practices and national security objectives.

The Committee will benefit from learning more about the types and numbers of transactions that may be circumventing CFIUS and if any are believed to have already transferred critical technology.

Many of us are interested in learning more about the ways China acquires U.S. technology and which improvements to the current system are warranted, particularly with regard to those investments that fall short of a foreign person's actual ownership or control.

We are also interested in the issue of emergent 'critical technology,' and the witnesses' input on how it would be defined and applied by CFIUS.

Additionally, we hope to hear more on the impact on U.S.-based multinational corporations as a result of CFIUS unilaterally restricting U.S. outward investment and associated technology, and whether U.S. companies would lose the ability to compete to allied companies or others in third-country markets.

It is also important to study the question of necessary resources for any proposed reform to CFIUS. While CFIUS certified about 260 applications last year, the Committee looks forward to testimony on the changes contemplated by S. 2098 and their impact on the number of reviews, staff needs and resources going forward, and the impact that, in turn, would have on U.S. national security if the resources fell short.

CFIUS is but one leg of a triad that secures national security related technology and the defense industrial base. The other two are the U.S. export control regime and Federal investment itself in research and development that keeps the industrial base resilient and innovative.

The Committee must be mindful that in pursuing its mandate to assure the national security interests of the United States under CFIUS, that it not create a situation where it chills a wide range of commercial activities that have traditionally been controlled through export control laws.

The United States is both the world's largest foreign direct investor and beneficiary of foreign direct investment (FDI), and it ranks among the most favorable destinations for FDI which plays an important role in not only the U.S. economy, but specifically in the innovation of its industrial base, and therefore, its national security.

It is clear that the current CFIUS system is itself under stress. Moving forward, the Committee must prepare itself to thoughtfully consider all of the recommendations made by S. 2098 and other CFIUS legislation, with the full awareness of the national security and economic stakes at the heart of it.

It is a new world. The laws, regulations and policies currently exercised by CFIUS may no longer protect U.S. technology from illicit transfers as they did in the past.

We must work together, as a Congress, first to assure the national security of the United States by granting the Administration all the authority it needs to confront this growing threat, but then not exceed that grant to the detriment of maintaining a free, fair and open U.S. investment policy."

PREPARED STATEMENT OF SENATOR JOHN CORNYN

JANUARY 18, 2018

Introduction

Thank you, Chairman Crapo and Ranking Member Brown, for convening this hearing to consider the proposal that Sen. Feinstein and I have put forward, the Foreign Investment Risk Review Modernization Act (FIRRMA). I have been honored to collaborate on this legislation with my esteemed colleague, Senator Feinstein, who I serve alongside on both the Judiciary and Intelligence Committees.

We spent many months working on FIRRMA, and we wrestled with some tough issues in the process. Based in part on the information we are exposed to on the Intelligence Committee, we believe these issues are urgent and complicated ones. The bill we have put together takes a targeted approach to addressing the problem, while also aiming to not unnecessarily chill foreign direct investment. Before we get into addressing the merits of the bill, however, I'd like to take a moment to highlight the list of people who have endorsed this legislation. That includes current U.S. national security leaders such as Secretary of Defense James Mattis; Secretary of the Treasury Steven Mnuchin; Attorney General Jeff Sessions; and Admiral Harry Harris, Commander of U.S. Pacific Command.

It includes former U.S. national security leaders such as former Secretaries of Defense Donald Rumsfeld and Bill Perry; former Secretary of Homeland Secretary Michael Chertoff; former Director of National Intelligence and Commander of U.S. Pacific Command, Admiral Dennis Blair; General Mike Hagee, former U.S. Marine Corps Commandant; General Edward Rice, former Vice Commander of Pacific Air Forces and Commander of U.S. Forces in Japan; and General J.D. Thurman, former Commander of U.S. Forces Korea and U.S. Army Forces Command.

The list includes private industry players such as telecommunications giant, Ericsson, Inc.; Oracle Corporation; Trinity Industries; Amsted Rail Company, Inc.; the Greenbrier Companies, the 20 member companies of the American Iron and Steel Institute; and the 260-member Railway Supply Institute. It includes China experts such as Dr. Larry M. Wortzel, a member of the U.S.-China Economic and Security Review Commission.

Mr. Chairman, with your indulgence, I encourage the Committee Members to review the comments of these supporters, and I ask consent to submit their letters and quotes for the record. I would also ask consent to submit for the record several summary and background documents on FIRRMA.

Context: China

The context for this legislation is important and relatively straight forward, and it's China. I have always been an ardent supporter of free trade, and I strongly support foreign direct investment in our country, consistent with the protection of our national security. However, the not-always-peaceful rise of China has significantly altered the threat landscape in recent years.

General Joe Dunford, Chairman of the Joint Chiefs of Staff, has said that by 2025, China will pose the greatest threat to U.S. national security of any nation. And, last summer, CIA Director Mike Pompeo echoed that view, saying that, over the long-term, China represents a graver security risk than even Russia or Iran.

It's not just that China poses a threat, though, it's that the kind of threat is unlike anything the United States has ever before faced—a powerful economy with coercive, state-driven industrial policies that distort and undermine the free market, married up with an aggressive military modernization and the intent to dominate its own region and potentially beyond.

To close the technology gap with the United States and leap-frog ahead of us, China uses both legal and illegal means. One of these tools is investment, which China has weaponized in order to vacuum up U.S. industrial capabilities from American companies that focus on dual-use technologies. China seeks to turn our own technology and know-how against us in an effort to erase our national security advantage.

In the modern era, the U.S. Military has always had a decisive technological advantage over our adversaries. This advantage is eroding before our very eyes, in

part because some U.S. companies have willingly helped China build industrial capabilities with clear national security applications. It is time to tackle the underlying problems head-on, while there is still time.

If the trend continues for the foreseeable future, what might this mean for our national security? We would potentially have an adversary that can dominate the cyber realm, defeat our space weapons, and control the skies as well or better than the U.S. Military. Just imagine if China's military was stronger, faster, and more lethal—such that China could unilaterally dictate which ships can transit through critical sea lanes in the Indo-Pacific region. Or, imagine if China could invade its democratic island neighbor Taiwan with impunity. The implications for the United States would be profound, both security-wise and economically. That is what the future likely holds, unless we act.

I encourage each Member of this Committee to get a classified intelligence briefing on these issues. I and my staff would be happy to set those up for you, if helpful.

Rationale and Key Objectives of FIRRMA

As it currently stands, the jurisdiction of the Committee on Foreign Investment in the United States (CFIUS) is quite limited; it was designed for the last century, not the present one. China has found gaps in both the existing CFIUS process and the export control system and is exploiting them to the detriment of our national security, aiding its own military modernization and simultaneously weakening our U.S. defense industrial base. FIRRMA takes a measured and targeted approach to close these gaps, with changes that are laser-focused on national security concerns. Its provisions also reflect the need to preserve as much certainty and predictability for investors as possible.

The rationale behind FIRRMA is simple: CFIUS should be able to review transactions that have, in effect, the same national security consequences as a traditional acquisition of a U.S. company or a piece of it. Foreign investors should not be able to circumvent CFIUS and get via the "back door" something they cannot get through the "front door."

To take advantage of these gaps and circumvent CFIUS review, China pressures U.S. companies into business arrangements such as joint ventures, coercing them into sharing their technology and know-how, enabling Chinese companies to acquire high-tech U.S. industrial capabilities and then replicate them on Chinese soil.

China has also been able to exploit minority-position investments in early stage technology companies in places like Silicon Valley, California, or the "Silicon Hills" in Central Texas to gain access to intellectual property (IP), trade secrets, and key personnel. The Chinese have figured out which dual-use emerging technologies are still in the cradle, so to speak, and not yet subject to export controls.

FIRRMA would expand the jurisdiction of CFIUS to cover some of these technology joint ventures and related arrangements and minority-position investments, as well as certain real estate transactions near military bases.

China's Civil-Military Integration Policies

The problems are compounded by some of China's carefully constructed policies on civil-military integration, under which China's military suppliers and their activities are woven right into China's commercial environment, unlike in our free market economy. To help modernize its military, China purposely blurs the lines between military and ostensibly commercial activities, combining its defense and civilian industrial bases. As such, U.S. technology and know-how transferred to "private" Chinese companies are likely to contribute directly and materially to China's military modernization.

Here, our export control system does not address the problem because the diversion of U.S. dual-use technologies is no longer just a risk, but a foregone conclusion. It is safe to assume that China will divert the fruits of any U.S. company's cooperation with China to a military end-use. It would be foolhardy to think these capabilities are not making their way into the hands of the Chinese military.

Further, U.S. companies doing business in China are entirely subject to the whims and dictates of the Chinese Communist Party. And, there is no real difference between a Chinese state-owned enterprise and a "private" Chinese firm, in terms of the national security risks that exist when a U.S. company partners with one. Rule of law in China is often illusory, and the Chinese Communist Party can easily exercise control over both types of companies, as American Enterprise Institute economist, Derek Scissors, has pointed out.

There are also major concerns regarding U.S. data, especially the personally identifiable information (PII) of U.S. citizens, and export controls do not cover this. The Chinese Communist Party considers data to be a national strategic resource, so

China is basically nationalizing all data. Therefore, when U.S. companies are forced to on-shore data into China, it can have major U.S. national security implications.

So, China is clearly not normal business environment for U.S. companies, and CFIUS modernization is the only way to effectively address the national security risks.

Debunking Arguments by Opponents of FIRRMA

I want to take a moment to debunk a few flawed arguments that some opponents of FIRRMA are making.

First, they say this bill represents regulatory overreach, which really misses the point. I am typically one of the loudest Senate voices of opposition to unnecessary regulation, as my track record demonstrates. But, this is very different—CFIUS is not akin to something like the Consumer Financial Protection Bureau; instead, it is part of our national security apparatus. And, the Federal Government has no higher duty than to maintain our national security.

Second, opponents claim that the export control system can already address these national security risks, and that this update to the CFIUS statute is unnecessary. Without question, export controls are vital in preventing transfers of technology that would be damaging to national security, and I am committed to maintaining a strong export control system. That is why under FIRRMA the export control system would remain the first line of defense when it comes to technology transfers.

Export controls work reasonably well in many cases, but they have inherent limitations and are not enough by themselves. We need a second line of defense. The CFIUS process and the export control system are designed to be interactive and complementary, not mutually exclusive. To effectively address the full range of mounting national security risks regarding China's activities, these systems must be robust, interoperable, and seamless.

Our bill certainly does not duplicate the export control system. With transactions that represent pure technology transfers—basically, just the IP—FIRRMA leaves those to the export control system. It would only cover certain outbound U.S. transactions where they also include the transfer of know-how, which is the so-called "secret sauce." These are the types of transactions that could help China acquire an industrial capability that is embodied in the U.S. business and accelerate China's learning curve in areas of technology that are key to national security.

What's more, FIRRMA includes safeguards to ensure that, with its expanded authorities, CFIUS would review transactions only when necessary. CFIUS would define circumstances in which transactions could be excluded because other provisions of law, such as export controls, are adequate to address any national security risks. This same provision also leaves ample room for future export control reform by giving CFIUS the flexibility to exempt transactions in the future that are adequately addressed through the export control regime.

CFIUS would also be authorized to create a "safe list" of certain allied countries, for which these new types of transactions would be exempt from review. This provision would drastically reduce the pool of transactions that would need CFIUS review, allowing CFIUS to focus its efforts on higher-risk deals.

Third, opponents argue that FIRRMA will flood and distract CFIUS with transactions that were previously routine. This argument questions whether addressing real national security threats is worth the financial cost; I assure you it is. For the price of a single B–21 bomber, we can fund an updated CFIUS process and protect our key capabilities for several years. That is a down payment on long-term national security. I am fully committed to securing the necessary funding for implementation to ensure the process continues to run smoothly, because this has to be a national security priority right up there with training and equipping our troops and intelligence professionals.

FIRRMA would also help provide additional resources, allowing CFIUS to charge modest filing fees and also submit a unified annual budget request covering all member agencies. And, the bill's own provisions guard against an unfunded mandate, with the expansion only taking effect after CFIUS determines on its own that the necessary personnel and other resources are in place. FIRRMA also exempts outbound transactions that are done through "ordinary customer relationships," ensuring harmless day-to-day activities do not have to be reviewed.

Closing

In closing, I also ask you to withhold judgment on FIRRMA until you have heard testimony from the Treasury Department and other key member agencies of CFIUS, who are on the front lines of this issue.

While it is certainly appropriate to consider what the potential impacts of this bill could be on foreign investment, that should not be done in a vacuum. We must also

ask what the impacts on our national security will be if we do not take action on this.

As you hear from opponents of FIRRMA, I urge you to assess their credibility on this issue by asking some basic questions about their activities in China:

- What types of arrangements do you currently have in China with Chinese companies, what do you have planned for the near future, and is CFIUS able to review any of it?
- What dual-use technology and know-how has your company transferred to China over the last decade, and what impact has that had on our country's relative national security advantage?

Increasingly, U.S. companies operating in China are being unfairly pressured into turning over valuable technology and know-how to Chinese companies, often as a condition of getting market access. Regardless, when U.S. companies engage in activities on Chinese soil that could negatively impact our national security, the Federal Government has a legitimate interest in being notified and afforded a chance to assess the national security risks. If CFIUS is not modernized to allow for this, we will continue to be in the dark here, and our national security will suffer.

I urge you to advance this bill for the sake of our long-term national security, which is being damaged before our very eyes. The time to modernize CFIUS is now, and we must not allow ourselves to be the frog in the boiling pot of water, so to speak.

Thank you, Mr. Chairman.

PREPARED STATEMENT OF SENATOR DIANNE FEINSTEIN

JANUARY 18, 2018

Chairman Crapo, Ranking Member Brown, thank you for inviting Senator Cornyn and me to your hearing to discuss the need for CFIUS reform. While I regretfully am unable to attend in person, I appreciate the opportunity to offer these written remarks.

I would like to open my remarks by commending this Committee for taking up this issue and its interest in identifying ways we can strengthen the United States' foreign investment process. We have heard for some time in the Intelligence Committee about the need for reform and the concerns regarding investment strategies other nations are employing to undermine our security.

When I was Mayor of San Francisco, we had a sister city relationship with Shanghai. Through this relationship I grew close with Jiang Zemin, then the Mayor of Shanghai. Eventually, Jiang Zemin became the President of China.

In this position, President Zemin prioritized efforts to privatize China's economy and, ever since then, there has been significant economic growth and development, including in foreign investment. In fact, in 2016, Chinese entities invested a record $46 billion in the U.S. economy, triple what they invested the prior year and 10 times what they invested 5 years ago.

While this growth has done much to improve and grow China's economy, it poses unique threats to United States national security.

For example, Chinese companies, often backed by the Chinese government, have increasingly used investment in U.S. businesses to acquire sensitive new technologies and related know-how. Many of these technologies, such as artificial intelligence and robotics, have military applications, and gaining access to such cutting-edge technologies has been a key part of the Chinese government's strategy to modernize its military.

Other investments threaten our national security because they allow China to acquire land or buildings in strategically sensitive locations—like near U.S. military bases or other Federal facilities. It's the job of the Committee on Foreign Investment in the United States—or CFIUS—to police foreign investment for national security concerns.

However, the current law governing CFIUS, including the scope of its authority, has not been updated for over a decade. In that time, China and other countries have begun structuring their investments in U.S. businesses so that they can evade CFIUS jurisdiction.

For example, many of these transactions take the form of joint ventures or minority-position investments, which CFIUS currently does not have the authority to reach. As a result, many transactions that pose potential national security concerns are going completely unreviewed.

In short, CFIUS just doesn't have the tools it needs to effectively screen foreign investments for these emerging national security threats.

The Foreign Investment Risk Review Modernization Act, which I am cosponsoring with Senator Cornyn, addresses these concerns.

First, it provides CFIUS with a new arsenal of tools to prevent foreign companies from evading its jurisdiction. Under current law, CFIUS may review only foreign investments structured as mergers, acquisitions, or takeovers. But our bill expands this authority, allowing CFIUS to reach joint ventures, minority-position investments, certain leasehold arrangements, and other investments where a foreign company effectively gains control of a U.S. business, regardless of how the transaction is structured.

Second, it streamlines the CFIUS filing process in an effort to encourage parties to notify CFIUS of potentially problematic transactions in the first place.

Third, our bill mandates that CFIUS place a greater focus on the threat posed by the transfer of cutting-edge technologies to foreign countries such as China. By redefining the term "critical technologies" to include these emerging technologies, the bill allows CFIUS to take into account the full range of national security concerns potentially posed by transactions that result in technology transfers to foreign companies.

Finally, our bill gives CFIUS additional flexibility to address national security concerns it identifies, granting CFIUS new authority to suspend transactions during its review and attach mitigation conditions to abandoned transactions when necessary. It also enhances CFIUS's ability to monitor and enforce mitigation measures and to take action when parties fail to comply with such measures.

In closing, I want to be clear, not all foreign investment causes national security concerns. Rather, the vast majority of such investment greatly benefits this country. Foreign investment has long been an important source of capital that supports U.S. innovation, economic growth, employment, and global competitiveness.

However, we must do all we can to ensure we can differentiate between the two.

That is why, for the past 10 months, Senator Cornyn and I have been working to craft a bill that strikes the right balance by giving CFIUS greater authority to address very real national security issues without unduly chilling foreign investment in the United States. By expanding CFIUS's authority in a targeted manner and granting CFIUS the flexibility to further define that authority through regulations, this bill does just that.

In fact, our bill has received support from several Federal stakeholders and members of the Intelligence Community.

In short, I think this is a strong bill that fills crucial gaps in the current CFIUS process. I hope you will join Senator Cornyn and me in supporting the Foreign Investment Risk Review Modernization Act.

PREPARED STATEMENT OF CHRISTOPHER PADILLA

VICE PRESIDENT FOR GOVERNMENT AND REGULATORY AFFAIRS, IBM CORPORATION; AND FORMER UNDER SECRETARY FOR INTERNATIONAL TRADE, DEPARTMENT OF COMMERCE

JANUARY 18, 2018

Mr. Chairman, Senator Brown and Members of the Committee, thank you for inviting me to testify on this very important topic.

My name is Christopher Padilla, and I am Vice President for Government and Regulatory Affairs at IBM. During the Administration of President George W. Bush, I served as Under Secretary of Commerce for International Trade, Assistant Secretary of Commerce for Export Administration, and in other senior roles in the Department of State and the Office of the United States Trade Representative.

In my Government roles, I was a senior sub-Cabinet representative of the Commerce Department to the Committee on Foreign Investment in the United States (CFIUS), and I participated closely in inter-agency work to implement new Committee procedures after passage of the Foreign Investment and National Security Act of 2007 (FINSA).

In my role at IBM, I have been involved in two large transactions that were reviewed by CFIUS, and am responsible for the company's worldwide compliance with export controls. My comments today draw upon all these experiences.

IBM shares Congress' goal of strengthening America's national security and appreciates the attempt to do so through the Foreign Investment Risk Review Modernization Act of 2017 (FIRRMA). CFIUS plays an important role in screening inbound foreign investments for potential national security risks, and it is necessary to periodically consider how this process can be improved.

In recent years, IBM has been through three reviews by CFIUS resulting in the successful conclusion of each transaction. From this experience, and from working on mitigation agreements when I served in Government, I can assure you that CFIUS has—and makes good use of—its authority to address potential security concerns about inbound foreign investment.

Nevertheless, these experiences also revealed the need for improvements to the CFIUS process, including an expansion of the Committee's jurisdiction to review certain types of inbound foreign investment transactions. FIRRMA contains some important reforms that IBM supports, such as:

- Expanding the ability of CFIUS to review a limited number of nonpassive, but noncontrolling, investments;
- CFIUS review of transactions when there are material changes in shareholder rights that expand control or access to information;
- Expanding the ability of CFIUS to review certain real estate transactions when they are in close proximity to military or Government installations;
- Taking steps to prevent the deliberate evasion of CFIUS review through complicated financial structures;
- Expanding consultation with allies to coordinate and share information on the types of inbound investment to be scrutinized;
- Ensuring there is a single Senate-confirmed appointee in each CFIUS agency with responsibility and accountability for investment reviews; and
- Providing badly needed resources to the Committee. The CFIUS case load has increased significantly in recent years, and staff resources are already stretched thin. Even if Congress does not elect to give CFIUS an expanded mandate along the lines noted above, it should provide additional resources for CFIUS to do its job effectively.

But the problem with FIRRMA, Mr. Chairman, and a principal reason the bill is controversial in the business community, is that it does something else: it would drastically expand the Committee's mandate beyond examining inbound investment. For the first time, CFIUS would review outbound international commercial activity, including many thousands of nonsensitive IP and technology licensing transactions, even with friendly nations.

This is a serious flaw in the bill that would duplicate and seriously undermine the existing U.S. export control regime, result in a flood of cases that would quickly overwhelm the Committee, and could constitute the most economically harmful imposition of unilateral trade restrictions by the United States in many decades.

Effectively Protecting National Security

As a company with long experience in foreign markets, IBM knows that controlling sensitive technology works best when accomplished internationally, in cooperation with America's allies.

Since the late 1940s, the United States has worked with other countries to stop sensitive technologies from falling into the wrong hands. Whether for dual-use goods like computers and electronics, or for chemicals, aeronautical products, missile technology or nuclear materials, Congress and the executive branch have recognized that to be effective, controls on technology should be multilateral.

A multilateral approach is important for a simple reason: the United States does not have a monopoly on smart people, advanced technologies or investment in leading-edge R&D. Many emerging, dual-use critical technologies are available from other countries, and companies and governments around the world continue to drive the frontiers of technology through their own R&D investments. In fact, in 2017, three-fourths of total global investment in R&D was conducted outside of the United States.[1]

A system of technology controls that unilaterally stops American firms from doing business abroad will not advance national security interests if it simply hands markets to foreign competitors—many of whom are equally capable in advanced technologies.

Yet this is precisely what FIRRMA would do. As drafted, the bill would impose a very onerous—and entirely unilateral—set of restrictions on outbound transactions of U.S. companies involving the "contribution" of technology, intellectual property, and associated support "through any type of arrangement."

---

[1] *2017 Global R&D Funding Forecast, R&D Magazine,* Winter 2017 (available at: *http://digital.rdmag.com/researchanddevelopment/2017_global_r_d_funding_forecast?pg=1#pg1.*

This is an exceptionally broad universe that would capture countless licensing, joint development, sales, research, and other transactions involving foreign persons, most of which involve technology that the U.S. Government previously determined did not warrant export control restrictions. For example:

- **Computer Hardware Sales & Service:** U.S. firms sell computers, servers and systems worldwide, often paired with installation, maintenance and technical support services. This hardware and related support typically involves hundreds of patented or licensed technologies that would count as a "contribution" of intellectual property under FIRRMA. For example, the sale of a computer server with tech support to a bank in Singapore could come under CFIUS review.
- **Software Licensing:** American technology companies license many types of software applications to both businesses and consumers. These applications often come with technical support that may include help desk, software updates, bug fixes and customization, all of which could involve patented or licensed technologies. For example, the licensing of a database application to a pharmaceutical company in Switzerland could be captured by FIRRMA.
- **Trademarks:** U.S. companies routinely license this most basic form of intellectual property to partners around the world for marketing and business development purposes. This bill could potentially trigger a staggering volume of regulatory filings for basic trademark deals that could not be less threatening to national security.

Saying that "ordinary customer relationships" are excluded would not solve this overreach, as that term, too, is undefined in FIRRMA and left entirely to the discretion of regulators. Neither is it comforting to be told that regulators will narrow the scope of covered outbound reviews after legislation is passed. Congress, not unelected officials, should decide how broad the CFIUS regulatory remit should be.

More practically, by covering such an extraordinarily broad range of transactions, CFIUS would quickly be overwhelmed with new reviews, making it difficult for the Committee to focus adequately on real threats to national security. Under FIRRMA, the CFIUS workload would skyrocket from about 250 cases per year—already a record number—to many thousands or even tens of thousands, including review of many routine outbound investments and technology transactions hitherto seen as nonthreatening by the United States and its allies.

Duplicative Regulation Would Harm U.S. Economic Competitiveness

As drafted, FIRRMA would turn CFIUS into a supra-export control agency, duplicating long-standing U.S. export control regimes and unilaterally limiting the ability of American firms to do business around the world. Foreign competitors that do not face similar regulatory restrictions will seize global market opportunities while American companies are left watching from the sidelines.

FIRRMA would give CFIUS extremely broad discretion to define the scope and reach of its regulatory authority, creating uncertainty and delays in investment decisions, contract negotiations and sales to foreign customers.

This approach stands in stark contrast to the approach recently taken by Congress and the Administration to curtail duplicative bureaucracy and regulation, and could capture under Government control a very wide range of commercial activity. As a result, foreign customers and investors will look elsewhere, and over the long term this could drive innovation and the development of new critical technologies outside the United States.

Protecting National Security Using Existing Authorities

One of the issues driving FIRRMA is a concern that the current CFIUS and export control regimes do not address the issue of emerging critical technologies. There is some justification for this concern. However, there is existing regulatory authority to impose new technology controls quickly, while also ensuring that effective, long-term controls are established in partnership with U.S. allies.

In 2012, a final rule was published (15 CFR 742.6(a)(7)) which established the "0Y521" series of controls in the Export Administration Regulations (EAR). Under this little-used regulation, the Government can impose immediate controls on emerging or other technologies if deemed in the national security or foreign policy interests of the United States. Crucially, however, this regulation also envisions that the United States will simultaneously pursue effective multilateral controls for these technologies with U.S. allies. And such controls would be administered through the specific, parameter-based, and relatively transparent process of export licensing that the business community knows and can work with.

So, mechanisms exist to quickly control sensitive technologies if necessary. But which technologies should be so controlled? This is where the picture gets murkier.

Technology control lists are badly in need of a refresh, and Congress should consider using its oversight authority to make this happen. Under the Export Administration Act, Congress directed that regular list review should be a priority, and it established the Militarily Critical Technologies List (MCTL) in statute for just that purpose. Yet a GAO report in February 2015 found that "the MCTL was out-of-date and was no longer being published online, but that widespread requirements to know what is militarily critical remained."[2] The same report found:

> According to DoD officials responsible for the MCTL, they are no longer updating the list, and are in the process of determining whether it is appropriate to seek relief from the requirement to maintain the list. They stated that alternatives to the MCTL are being employed based on the specific needs of each agency, and DoD offices are using the U.S. Munitions List, the Commerce Control List 600 Series, and the Industrial Base Technology List as alternatives to the MCTL.[3]

This is not how Congress thought the process should work. Using the control list to say what is militarily critical puts the cart before the horse. The intent was that the Defense Department, working with other agencies and with industry, would broadly identify general categories of militarily critical technologies (including emerging technologies of concern) in the MCTL, and then draw from that list to propose specific, parameter-based, and usually multilateral export controls. The controls would be implemented via the Commerce Control List, the U.S. Munitions List, and international control regimes such as COCOM (succeeded by the Wassenaar Arrangement), the Missile Technology Control Regime, the Australia Group, the Nuclear Suppliers Group, or others. Export controls have worked well to protect national security for decades, but the list review process has recently fallen into disuse.

FIRRMA would not correct this problem, and in fact could make it worse. Under FIRRMA the Government would define some new, very vague and broad list of technologies of concern (even though it has failed to update technology lists already required under current law) and then wait until something pops up in a transaction review. The Government might then try to stop it—but only unilaterally, on a deal-by-deal basis, and without regard to foreign availability, technology trends, or consultation with allies or industry. Casting an extraordinarily wide net over routine commercial transactions and applying, in effect, a regulatory test of "we'll know it when we see it" would be deeply damaging to U.S. competitiveness, and, more important, could lead to a false sense of security.

Instead, there should be a return to a more disciplined list review and multilateral export control process already mandated by law. Congress could act to ensure effective monitoring and control of emerging technologies through existing export regulations by requiring:

1) regular, ongoing reviews of emerging technologies for potential national security risks as envisioned by the MCTL;
2) full and robust application of existing EAR regulatory authorities to control these emerging technologies as necessary to protect national security; and
3) annual reports to Congress with additional oversight to ensure that this export control process effectively addresses any risks.

Conclusion

In summary, IBM fully supports efforts to strengthen national security. We encourage Congress to find ways to do so without undermining U.S. economic competitiveness, or driving innovation and investment outside the United States.

We believe that a refreshed technology control list, and the more robust use of existing export control authority ultimately leading to international controls, would be the most effective way to protect national security interests.

While FIRRMA contains several important reforms to CFIUS, the Committee should continue to focus on inbound foreign investment in the United States, rather than reviewing outbound transactions that are low-risk or already covered under existing export control regulations.

---

[2] U.S. Government Accountability Office, *"Critical Technologies: Agency Initiatives Address Some Weaknesses, But Additional Interagency Collaboration is Needed,"* February 2015, GAO 15–288.

[3] Ibid., and reference is also made to a prior report: U.S. Government Accountability Office, *"Protecting Defense Technologies: DoD Assessment Needed to Determine Requirement for Critical Technologies List,"* January 2013, GAO–13–157.

Thank you for this opportunity to appear before the Committee. I would be pleased to answer any questions that you might have.

Written Testimony of Scott Kupor
Managing Partner, Andreessen Horowitz
Chair, National Venture Capital Association
before the U.S. Senate Committee on Banking, Housing, & Urban Affairs
"CFIUS Reform: Examining the Essential Elements"

January 18, 2018

Chairman Crapo, Ranking Member Brown, thank you for the opportunity to testify before the Senate Banking Committee regarding reforms to the Committee on Foreign Investment in the United States (CFIUS) and the *Foreign Investment Risk Review Modernization Act of 2017* (FIRRMA, S. 2098). My name is Scott Kupor and I serve as Managing Partner of Andreessen Horowitz, a $7 billion dollar venture capital firm that has invested in many early-stage technology companies, such as AirBnB, Lyft, Oculus, Pinterest, Coinbase and Instacart. I am testifying in my capacity as Chair of the National Venture Capital Association (NVCA).

As detailed below, the basic business model of venture firms is to raise capital from a diverse set of investors to invest in startups. Some of these investors (which we refer to as limited partners, or LPs) are from abroad, as foreign investors seek returns from venture investing in the same way that U.S. investors have for years. While U.S.-based universities and endowments have been – and continue to be – important limited partners in venture capital funds, increasingly non-U.S. investors are seeking to deploy capital in U.S. venture funds as a means of generating above-market returns. I believe that policymakers should encourage, and not be fearful of, foreign investment into U.S. venture funds.

The U.S. has a very strong entrepreneurial mindset, world-class research universities that help engender forward-thinking research and development, and an incredibly strong talent pool of individuals seeking to build new technology-based businesses. Developing these businesses – the benefits of which will accrue to the U.S. in terms of employment, economic growth, and increases in the overall standard of living – requires risk capital; thus, it is imperative that we retain a robust venture capital financing ecosystem in the U.S. and continue to attract non-U.S. dollars. If we create obstacles to the investment of these dollars in the U.S., they will simply go to other countries. The other countries that receive these dollars may make gains in defense-related technologies, along with other attendant benefits that come along with new company formation.

In fact, to illustrate this, the U.S. venture capital industry represented about 90% of global venture capital dollars in 1990; today, that global market share has been reduced to 54%.[1] To ensure that we as a country maintain our global technology lead, we should make sure that the U.S. venture capital markets remain open and attractive to non-U.S. players. Other countries are eager to take advantage of any obstacles we place to the free flow of risk capital in the U.S. to further their own attractiveness to global investors.

[1] Pitchbook – NVCA data.

The U.S. venture capital industry stands ready to work with the Senate Banking Committee and the authors of *FIRRMA* to ensure the legislation does not produce unintended consequences that may be harmful to new company creation in the United States.

Venture capital and its importance to the U.S. economy

The story of venture capital (VC) is really a subset of the story of entrepreneurship. As venture capitalists, we raise investment funds from a broad range of LPs, such as endowments, foundations, pension plans, family offices, and fund-of-funds. The capital raised from LPs is then invested in great entrepreneurs with breakthrough ideas. Venture capitalists invest anywhere from the very early stage, where the startup has little more than an idea and a couple of people, to growth-stage startups, where there is some revenue coming in and the focus is on effectively scaling the business. Generally, a company leaves the venture ecosystem via an initial public offering (IPO), a merger or acquisition, or bankruptcy.

There is often a misconception that venture capitalists are like other investment fund managers in that they find promising investments and write checks. But writing the check is simply the beginning of our engagement; the hard work begins when we work with startups to help entrepreneurs turn their ideas into successful companies. For example, we often work with our companies to help them identify talented employees and executives to bring into the company or to identify existing companies who can serve as live customer test sites for their products.

The reality is that those who are successful in our field do not just *pick* winners. We work actively with our investments to help them throughout the company-building lifecycle over a long period of time. We often support our portfolio companies with multiple investment rounds generally spanning five to ten years, or longer. We serve on the boards of many of our portfolio companies, provide strategic advice, open our contact lists, and generally do whatever we can to help our companies succeed. While we hope that all of our companies succeed against huge risks and grow into successful companies, the reality is that the majority fail. As this committee appreciates, entrepreneurship is inherently a risky endeavor but it is absolutely essential to the American economy.

Successful venture-backed companies have had an outsized positive impact on the U.S. economy. According to a 2015 study by Ilya Strebulaev of Stanford University and Will Gornall of the University of British Columbia, 42 percent of all U.S. company IPOs since 1974 were venture-backed.[2] Collectively, those venture-backed companies have invested $115 billion in research and development (R&D), accounting for 85 percent of all R&D spending, and created $4.3 trillion dollars in market capitalization, 63 percent of the total market capitalization of public companies formed since 1974. Specific to the impact on the American workforce, a 2010

[2] "The Economic Impact of Venture Capital: Evidence from Public Companies," Stanford University Graduate School of Business Research Paper No. 15-55, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2681841.

study from the Kauffman Foundation found that young startups, most venture-backed, were responsible for *almost all* the 25 million net jobs created since 1977.[3]

It is quite clear that the American economy is dependent on the economic activity that comes from young firms scaling into successful companies. The rapid hiring, innovative product development, increasing sales and distribution needs, and the downstream effects all serve to push the U.S. economy forward. The American economy needs more of this activity to help deal with many of the challenges we see today. Historically, the United States has done an excellent job encouraging risk-taking and entrepreneurship, but it is imperative that policymakers, entrepreneurs, and VCs work together to encourage entrepreneurship in our country.

Challenges to American Leadership

The story of modern venture capital began in the U.S. and, as a country, we have been the predominant funder of most startup ventures. But other countries see the benefits that entrepreneurship has brought to the American economy and are increasingly competing with the U.S.

Increased interest in startups by other countries has caused the share of global venture capital invested in the U.S. to fall from 90 percent to 54 percent in only 20 years.[4] Foreign investment in the U.S. economy is the focus of this hearing, but it is important to note the degree to which startups in *other* countries are now attracting capital, and how innovation and entrepreneurship has become a global competition. There are undoubtedly justifiable concerns about China trying to procure sensitive technology through U.S. investment, but the reality is today they are building first-rate technology themselves. China attracted $35 billion in venture investment in 2016 and is now the second largest destination in the world for venture capital. In 2016, six out of the ten largest venture deals in the world occurred in China.[5] It is therefore critical that policymakers spend time solidifying our leadership position in entrepreneurship through regulatory changes, more effective startup tax policy, immigration reform, and increased investment in basic research.

Foreign investment in U.S. startups and venture funds is challenging to quantify

Because VC is a form of private capital, tracking exact sources of capital is nearly impossible. LPs, VCs, and startups all keep records of the investments they have made and/or received but are typically not required to publicly report these details. Except for public pension funds or other LPs mandated to do so, LPs generally do not publicly release information on their fund investments. Some VC funds publicly share the total fund size, date, and focus of a recent fundraise via a press release, their websites, or media interviews but rarely publicly disclose who are their LPs. Similarly, a startup may choose to publicly disclose a recent funding round, the amount of capital raised, and/or the participating investors, but the amount each investor

---

[3] http://www.kauffman.org/~/media/kauffman_org/research%20reports%20and%20covers/2010/07/firm_formation_importance_of_startups.pdf.

[4] Id.

[5] Id.

contributed is generally not shared. For these reasons, attempts to quantify the dollar amount of 1) foreign investment into U.S. VC funds, or 2) foreign entities direct investment into U.S. VC-backed startups are limited and unreliable.

Thus, while we do know that globally LPs committed approximately $142 billion to U.S. VC funds from 2014 to 2017,[6] we do not have precise figures indicating how much of these LP dollars are from Chinese and other foreign LPs. As a practitioner in the venture capital industry and the managing partner of a set of funds that have a diverse set of U.S. and non-U.S. LPs, I do believe that the amount of Chinese LP investment in U.S. venture capital firms is very small. I would estimate that fewer than 5% of total U.S. LP commitments are from Chinese LPs, and, anecdotally, I believe that most of that money is from private family offices or the large Chinese consumer internet players and not from Chinese government-related entities. There is a more robust non-U.S. ecosystem of venture capital LPs in other geographies, *e.g.*, Singapore, Western Europe, and the Middle East.

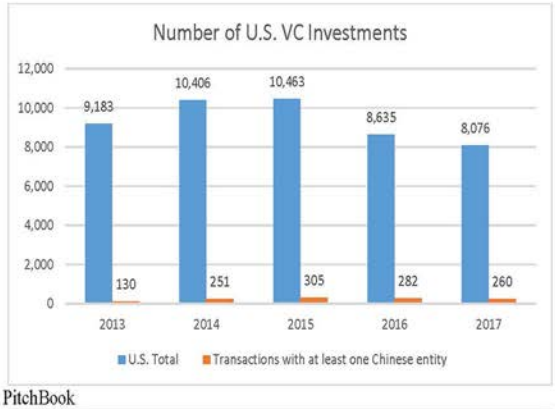
In addition to LP commitments, commercial data providers also track direct investment into U.S. VC-backed startups. These providers capture the funding round amount, the date the round closed, and the names of some, if not all, of the participating investors. Using this information, databases can crosscheck the location of the investor to determine its headquarters, therefore relatively accurately capturing the number of investments where at least one Chinese investor participated (see below). Because these sources report only the total amount of funding (vs. the amounts specifically contributed from a Chinese investors), they materially overstate the amount of foreign investment. For example, if a startup closes a $50 million fundraising round and a Chinese entity contributed $10 million of the capital, this might be reported as $50 million transaction that a Chinese entity was part of since it is not known that the Chinese entity contributed only 20 percent of the capital for that round. Given these limitations, I would encourage policymakers to exercise caution in using these estimates as a key rationale for supporting legislation or regulatory changes.

Using this methodology, we know that in 2017, U.S. venture-backed startups raised $84 billion across 8,076 transactions, of which 260, or 3.2 percent of all deals, included at least one Chinese entity.[7] These 260 transactions had an aggregate deal value of $9.3 billion, which includes capital from all investors (again, not only Chinese entities).[8]

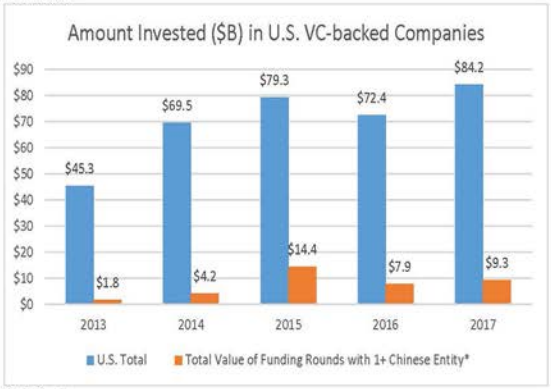
[6] "Record Unicorn Financings Drove 2017 Total Venture Investments to $84 Billion, the Largest Amount Since Dot-Com Era," *available at* https://nvca.org/pressreleases/record-unicorn-financings-drove-2017-total-venture-capital-investments-84-billion-largest-amount-since-dot-com-era/

[7] Id.

[8] PitchBook data as of January 2018, *available at* https://my.pitchbook.com/page/search_15568677



Source: PitchBook



Source: PitchBook
*Total value of funding round includes capital invested by Chinese entities and non-Chinese entities.

Again, as a practitioner in the industry, I believe that these numbers materially over-state the true amount of Chinese capital being invested into U.S. startups. The nature of VC funding rounds – particularly the later-stage rounds where non-US investment is more likely – is that they often include multiple investors. Often a "lead" investor – the one who negotiates the principal terms and often takes a board seat in connection with the investment – will contribute 50% of the investment amount, with the remainder often coming from additional new investors and/or from existing investors in the company. Thus, even if we assumed that Chinese investors were the lead investors in financial rounds totaling $9.3 billion, the contribution of the Chinese investor alone is likely no more than half of that total reported number, or $4.65 billion. Based on my experience in the industry, it is very unlikely that Chinese investors were the lead investors in all

of these rounds; thus, the total amount of Chinese investment is probably materially less than the estimated $4.65 billion.

In addition, as is the case with the Chinese limited partners, the vast majority of direct Chinese investors are either private family offices or private consumer internet companies (*e.g.*, Baidu, Alibaba and Tencent) – not Chinese sovereign money. Thus, the Chinese government is not likely a material investor in venture-backed U.S. companies.

Structure of VC funds mitigates concerns over Chinese investment

The venture capital industry shares the goal of this committee and *FIRRMA* to protect U.S. innovation and ensure that U.S. critical technology is not used to harm our competitiveness or security. It is important to understand, however, that the structure of VC funds effectively protects sensitive information of startups from disclosure to investors into the fund.

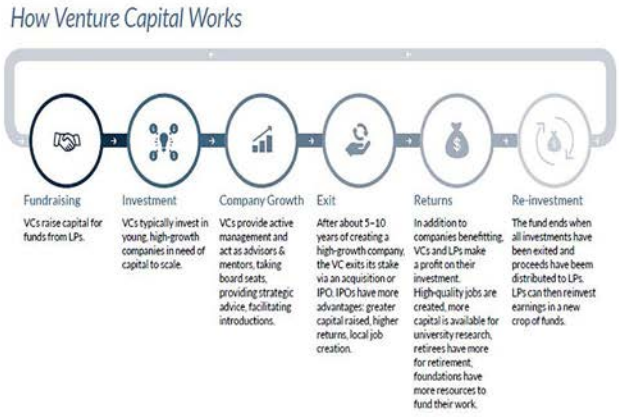
By way of background, the relationship between the investors in venture capital funds, LPs, and the individuals charged with managing the fund and making investments (general partners, or GPs) is governed by a limited partnership agreement (LPA). The LPA defines not only the economic relationship between the parties, but also the nature of involvement of the LPs in the investment entity. By design, the LPs have in fact very limited rights in the ongoing fund entity – they are expressly entitled to defined economics resulting from the investments and to regular financial reporting from the fund – but have no say in investment decisions and no ability to garner portfolio company information other than at the discretion of the GPs. In addition, the LPA contains a confidentiality provision that binds the LP to maintain in confidence all such information as provided by the GP. Thus, as a matter of course, information disclosure to LPs is minimal and largely related to valuation and accounting-related information to ensure that the LP understands its current economic position in the fund.

In most cases, venture capitalists will sit on the board of directors of the companies in which they invest and, as a result, will also owe duties of confidentiality directly to the shareholders of those companies. Thus, to the extent a venture capitalist were aware of proprietary technology in use or being developed by the company, she would not be in a position to share that with LPs. In fact, most LPAs have an express provision in them in which LPs acknowledge that GPs may have independent fiduciary duties to their companies such that they may be restricted in being able to share any information with LPs.

Thus, as a matter of common practice in the industry, most GPs provide LPs with quarterly financial reports of the fund's performance and, in some cases, investment letters that highlight interesting trends/new investments on which the GP may be focused. In my experience, in no case will those updates include details on intellectual property or other proprietary information – as noted above, not only might that violate the GP's duties to the company, but it would be against the financial self-interest of the GP to risk disclosing information that might leak to the marketplace and risk impairing the financial value of the asset.

GPs also typically host an annual in-person meeting for their LPs. These meetings generally are comprised of financial updates on the various investment funds and presentations from the GPs

on areas of investment focus for the firm. Some annual meetings will also include a few entrepreneurs from the portfolio, who will provide an overview of the company they are building. These are naturally high-level presentations focused on the market opportunity and do not include any meaningful disclosures on sensitive technology or intellectual property. For example, a company might disclose that it is seeking to create a drug to slow down the aging process by using machine learning techniques, but it would not describe any of the details of the technology. Again, the reason for this is quite simple – the companies go to extreme measures to maintain the confidentiality of their intellectual property, so any general disclosures can create risk.



FIRRMA should be improved by changes that will avoid unintended consequences

FIRRMA is well meaning legislation intended to deal with a real challenge. However, as drafted *FIRRMA* produces many questions about the filing obligations of U.S. venture capitalists when a fund has *any* amount of foreign LPs. *FIRRMA* also raises significant questions when a U.S. startup accepts foreign investment, even if that investment is for a small stake in a startup or when co-investing with U.S. investors. We appreciate the opportunity to work with this committee and *FIRRMA*'s sponsors to modify the bill in key ways that keeps in place its intended effects while avoiding serious issues for startups and venture capitalists.

Ambiguity in FIRRMA's impact on VC funds should be clarified

As drafted, *FIRRMA* is ambiguous in its application to a venture capital fund with foreign LPs. *FIRRMA* appears to be written with foreign direct investment in mind, *i.e.* a scenario where a

foreign person invests capital directly into a company.[9] The legislation does not specifically speak to the common practice of a foreign person that invests in a U.S. venture fund, which *in turn* invests in a critical technology company. We are concerned that this ambiguity—especially when combined with a broad grant of rulemaking authority to CFIUS—will cause unnecessary confusion, cost, and burden for the venture capital industry, as venture firms will be left without a clear understanding of whether they must file with CFIUS and under what circumstances.

We recommend *FIRRMA* be amended to clearly specify that U.S. venture funds with foreign LPs are not implicated by the covered transaction definition, nor does the fund take on foreign personhood for purposes of *FIRRMA* merely because it has foreign LPs. This crucial clarification is in line with the spirit of the bill, which importantly removes 'passive investment' from the definition of a covered transaction.[10] As detailed above, LPs in VC funds are by definition passive investors and therefore more should be done to provide clarity in this regard.

The ambiguity of *FIRRMA* causes concern that venture funds would need to file with CFIUS as a precautionary measure merely because it has a partially foreign LP base and *might* invest in a U.S. critical technology company in the future. This would be an unfortunate distraction from supporting the development of new startups. It would also be a bizarre outcome because when a VC fund is raised it is impossible to know whether the fund will ultimately invest in a 'critical technology' company. After all, a VC fund lasts approximately a decade and invests in new enterprises that in the vast majority of cases do not exist at the time the fund is raised. This can be contrasted with a foreign person that invests directly in a U.S. critical technology company, as the foreign person will likely know whether that company is 'critical technology' under *FIRRMA* at the time of the investment. It would also be distracting, inefficient, and nonsensical if a venture fund were required to file with CFIUS each time it made an investment in a startup out of its fund with foreign LPs. Startups move quickly and are in need of capital to scale their business. It would be impractical if a VC fund needed pre-clearance from the government before it provided that capital. I understand from CFIUS practitioners that CFIUS clearances can take four months or more from the time the parties begin working on the filing – that is not a time frame compatible with venture investing.

FIRRMA should not stifle foreign strategic investors that have become a key aspect of startup financing

A growing and important component of startup financing is participation by so-called foreign strategic investors, like investment arms of multinational corporations. These investors are increasingly providing capital to U.S. startups alongside U.S. venture funds as co-investors, especially in later-stage deals where the amount of capital raised by the company is significantly larger than would be raised by an early-stage company. These foreign strategic investors are important to the entrepreneurial ecosystem because frequently when a startup is raising capital

[9] Sec. 3(a)(5)(B(iii) of *FIRRMA* specifies that a "covered transaction" is *inter alia* an "investment (other than a passive investment) by a foreign person in any United States critical technology company or United States critical infrastructure company, subject to regulations prescribed under subparagraph (c)."
[10] *FIRRMA* Sec. 3(a)(5)(B(iii) and Sec. 3(a)(5)(D).

there will be multiple entities that will participate in the round as co-investors to ensure the startup is able to raise the capital it needs to grow.

It would be an unfortunate outcome if the foreign co-investor of a U.S. VC fund needed approval from CFIUS to participate in an investment round, as that would complicate and slow the round *even* in situations where the foreign investor is taking a minority stake in a round for a minority stake of the company. For example, imagine a U.S. critical technology startup that is raising capital from four entities, three of which are U.S. VC funds and the fourth of which is a foreign strategic investor. In that round, the company sells 20% of the company for $50 million and the foreign investor takes 25% of the round, resulting in a 5% ownership interest in the company. With a 5% ownership stake, the foreign strategic investor will not have access to sensitive information that is the concern of *FIRRMA*, but it may need to file preemptively with CFIUS out of caution to determine whether the investment is acceptable. Ideally, the foreign strategic investor would clearly meet *FIRRMA*'s passive investment test and be assured the investment was acceptable, but unfortunately that test is quite narrow and it will be a judgment call for the investor as to whether they qualify. This could result in a U.S. startup missing out on key investment capital as the company seeks to grow. As a practical matter, investment rounds are generally very competitive and decisions often are made in a matter of weeks if not days. Thus, filing requirements (or uncertainty) that would jeopardize this timeline are likely to mean that the investors will be prohibited outright from participating in the investment opportunity.

To avoid this situation, *FIRRMA* should specify that a CFIUS filing is not needed if the foreign strategic investor takes a *de minimis* stake in the startup (such as in the hypothetical above), as in that scenario the foreign strategic investor is a *de facto* passive investor but might fear it does not meet the tightly drafted passive investment text. Another helpful change would be to broaden the passive investment test to provide assurance to foreign strategic investors that they are not implicated by *FIRRMA*.[11] For example, the requirement that a foreign person not receive more "nontechnical information" than other shareholders should be modified, as this information is immaterial to the aim of *FIRRMA*.[12] Our industry would be pleased to work with *FIRRMA*'s authors and the Banking Committee to provide further detail on how this section can be improved.

FIRRMA should give CFIUS additional authority to exempt additional countries

FIRRMA grants CFIUS the authority to exempt countries from the definition of a 'covered transaction' if the country meets certain requirements. One factor CFIUS is directed to consider is "whether the United States has in effect with that country a mutual defense treaty."[13] This factor should be broadened to capture a wider universe of U.S. strategic partners that ought to be exempted from the covered transaction definition, as many of these countries are important sources of capital for high-growth U.S. companies.

[11] *FIRRMA* Sec. 3(a)(5)(D).
[12] Id.
[13] *FIRRMA* Section 3 (a)(5)(C)(ii)

Conclusion

Our industry appreciates the interest the Banking Committee and *FIRRMA*'s authors have paid to this important matter for national security. We encourage policymakers to proceed deliberately and with caution as it tackles this issue. As my testimony demonstrates, the modern startup investing ecosystem is complex and care should be taken to ensure it is not disrupted in a way that harms the ability of startups to grow. Our industry stands ready to work with policymakers as reforms to CFIUS are concerned.

PREPARED STATEMENT OF GARY CLYDE HUFBAUER, PH.D.*

REGINALD JONES SENIOR FELLOW, PETERSON INSTITUTE FOR INTERNATIONAL ECONOMICS

JANUARY 18, 2018

Thank you, Senator Crapo, and Members of the Committee for inviting me to testify concerning S. 2098, the Foreign Investment Risk Review Modernization Act of 2017. My remarks will also touch on the House counterpart legislation, H.R. 4311, the Foreign Investment Risk Review Modernization Act of 2017.

Two empirical facts provide the starting point for my remarks:

- Inward foreign direct investment is almost always good for the United States. Foreign firms that invest in the United States—usually by acquiring U.S. firms—are typically top of their class abroad. They pay higher wages than average U.S. firms in the same industry, do more R&D and investment, and export a larger share of production.[1] These facts are just as characteristic of Chinese firms as foreign firms based in Canada, Europe, or Japan.
- Outward foreign direct investment also benefits the United States. Contrary to popular mythology, investment abroad does not, as a rule, take place at the expense of investment in the United States. Instead, U.S. firms that invest heavily abroad typically grow U.S. R&D faster, employ more workers, and produce and export more than comparable U.S. firms that invest little or nothing abroad.[2]

Given these facts, the burden of proof should rest on any Government action that seeks to restrict either inward or outward foreign direct investment (FDI). Historically, this is how the Committee on Foreign Investment in the United States (CFIUS) has operated.[3]

CFIUS was created in 1975 to screen foreign takeovers of U.S. firms for threats to U.S. national security. The focus was on inward investment and technology acquisition. Treasury chairs the CFIUS, ensuring that the economic benefits of inward foreign investment are given due consideration, a perspective buttressed by membership of Commerce and USTR, and observer status of OMB, CEA and the NEC.

The CIA, NSC, and Defense fully inform other Committee members of the national security dimensions of any takeover. However, an influential draft report by Brown and Singh (February 2017) calls upon Congress to vest the power to block a transaction in just three Cabinet members, if they are all in accord: Defense, Justice and Homeland Security.[4] In the past, less than five takeovers have been blocked by CFIUS, but somewhat more applications have been withdrawn prior to an adverse decision. The Brown and Singh draft report advocates more stringent screening, especially with respect to Chinese transactions.

If enacted, the blend of S. 2098 and H.R. 4311 would significantly enlarge the CFIUS mandate to cover outward investment and technology transactions by U.S. firms. It would also cast a skeptical eye toward investment (inward or outward) from or to China, Russia, and a handful of other adversarial nations.

The new and broader CFIUS mandate raises three inter-related concerns:

- It could replace multilateral cooperation with unilateral restrictions on outward flows of "critical technology" to neutral or adversarial nations;
- Thereby putting U.S.-based multinational corporations (MNCs) at a disadvantage, relative to MNCs based in Europe or Japan, when firms compete in third-country markets;

---

*This testimony is based on a blog posted on the Peterson Institute website: *https://piie.com/blogs/trade-investment-policy-watch/revamping-cfius-and-going-too-far.*

[1] Theodore H. Moran and Lindsay Oldenski. 2013. *Foreign Direct Investment in the United States: Benefits, Suspicions, and Risks with Special Attention to FDI from China.* Policy Analyses in International Economics 100. Washington: Peterson Institute for International Economics. Also see Moran's remarks at *https://piie.com/system/files/documents/moran201702draft-c.pdf.*

[2] Gary Hufbauer, Theodore Moran, and Lindsay Oldenski. 2013. *Outward Foreign Direct Investment and U.S. Exports, Jobs, and R&D: Implications for U.S. Policy.* Policy Analyses in International Economics. Washington: Peterson Institute for International Economics.

[3] For a detailed background, see James K. Jackson, "The Committee on Foreign Investment in the United States (CFIUS)," Congressional Research Service, October 11, 2017.

[4] Michael Brown and Pavneet Singh, "China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of U.S. Innovation," pre-Decisional draft, Defense Innovation Unit Experimental, February 2017.

- And duplicate controls on the export of merchandise and technology established under the Export Administration Act with multilateral consultation.

Using existing statutory authorities, President Trump could achieve the objectives sought by S. 2098 and H.R. 4311. If he wants to restrict U.S. investment and technology flows to China, Russia, Iran or any other country, Trump can do so without new legislation.[5]

The lasting impact of these bills will come when a different president resides in the White House. If the CFIUS mandate is expanded as the co-sponsors contemplate, the CFIUS caseload will burst from 200 annually to thousands. Necessarily, the bureaucracy will blossom with new administrative and technical capabilities. Once the bureaucracy is created, and reviews become a thrice-daily event, it will be almost impossible to turn the clock back to today's open regime for investment and technology flows.

Under S. 2098 and H.R. 4311, future decisions to block inward or outward foreign direct investment might not require the Government to carry the same burden of proof as historically has been the case. Hypothetical arguments that allowing an acquisition or transferring certain technology abroad might in the future endanger national security will have greater weight. Proof may not be needed that the acquisition or transfer currently endangers national security. The cited Brown and Singh draft report, if followed, makes the change in emphasis very clear.

In fact, S. 2098 states, among other factors to be considered, "the potential effects of the covered transaction on United States international technological and industrial leadership in areas affecting national security, including whether the transaction is likely to reduce the technological and industrial advantage of the United States relative to any country of special concern."

Likewise, H.R. 4311, states, among factors to be considered, "whether the covered transaction is likely to contribute to the loss of or other adverse effects on technologies that provide a strategic national security advantage to the United States."

In plain language, both bills stipulate that any transaction that might enable a foreign country (especially an adversary) to narrow its gap with U.S. technological leadership should be viewed skeptically. This warning covers a great deal of ground, not only with respect to transactions with adversaries, but also with respect to transactions with neutrals or allies who might in turn convey the technology to adversaries.

Chinese technology practices have generated the core motivation for S. 2098 and H.R. 3411. China has targeted several high-tech industries for massive upgrading in the next 10 years. Multiple Chinese means of accessing frontier U.S. technology in an effort to achieve this goal are spelled out in the Brown and Singh draft report. Among other means, China acquires venture capital stakes in nascent technologies and compels foreign firms to transfer technology to Chinese business partners as the "price of admission" to the vast Chinese market. President Trump has directed the U.S. Trade Representative to launch an investigation of China's technology transfer practices, under Section 301 of the Trade Act of 1974. Once the investigation is concluded, measures to block U.S. firms from acquiescing to Chinese demands could be Trump's response, whether or not a blend of S. 2098 and H.R. 4311 passes Congress.

Both S. 2098 and H.R. 4311 refer to China, Russia and other U.S. adversaries as "countries of special concern" without naming them. CFIUS is directed to scrutinize inbound and outbound investment and technology transactions with these countries. At the same time, both S. 2098 and H.R. 4311 would allow CFIUS to exempt from review "covered transactions" with foreign firms based in countries that are U.S. military allies or have close security relations.

Recommendations

Legislation enacted by Congress should be narrowed to cover the immediate problem—transfer of critical technology to adversarial countries—without a massive expansion of the CFIUS mandate to review the bulk of outward foreign direct investment by U.S. firms.

Narrowing could be accomplished with two provisions. First, require the Committee to identify "critical technologies", drawing on the resources of the intelligence community, the National Academy of Sciences, and the National Academy of Engineering. Second, require the Committee to name "countries of special concern". With these two provisions, the workload would be narrowed while U.S. firms that develop

[5] The president can restrict foreign investment and exports of goods and technology under the International Emergency Economic Powers Act (IEEPA) and other statutes.

critical technologies would be put on notice to seek CFIUS review prior to transferring the know-how to worrisome countries.

CFIUS review of questionable transactions should take into consideration the availability of equivalent critical technology from firms not based in the United States. Obviously, if an end run through Europe or Japan has already occurred, there's less reason to block the U.S. firm. If an end run is only a future possibility, then a decision to block the transaction should be accompanied by a forceful diplomatic demarche to U.S. friends and allies to establish a multilateral basis for the denial.

Thank you for the opportunity to testify.

Statement before the
Senate Committee on Banking, Housing, and Urban Affairs
"CFIUS Reform: Examining the Essential Elements,"

A Testimony by:

James Mulvenon, Ph.D.
General Manager, Special Programs Division
SOS International

January 18, 2018

538 Dirksen Senate Office Building

Introduction and Main Points

Chairman Crapo, Ranking Member Brown, and distinguished members, thank you for inviting me to testify today.

In 2013, two U.S. government colleagues and I published a book entitled *Chinese Industrial Espionage*, which documented the efforts, both quasi-legal and illegal, used by the Chinese government and state-owned entities to steal U.S. technology, intellectual property, and secrets.[1] For me, this culminated almost two decades of tracking Chinese cyber espionage and the PRC military and defense industrial base's efforts at illicit technology transfer.

The current main problem as I see it is two-fold. One, the Chinese government has a comprehensive strategy for national economic growth and technology modernization. This strategy has created an unfair, asymmetric business environment in China, sometimes forcing American companies, who need to be in the China market to grow and prosper, to make suboptimal decisions that are not always in the long-term interests of U.S. national security, but clearly benefit Chinese national security. Two, U.S. laws and regulations governing Chinese investment in the United States, U.S. company technology transfers, and export controls have not evolved sufficiently to deal with Beijing's aggressive and constantly evolving strategy. In fact, early successes in the Committee for Foreign Investment in the United States (CFIUS) process in preventing inappropriate acquisition deals, such as the rejection of the Huawei-3COM deal, led Beijing to conclude that overt acquisition efforts, while preferred, would not always succeed, and led Chinese entities to adapt from outright acquisition to joint ventures and other investment vehicles typically outside the current CFIUS scope, using the power of access to the China market to leverage technology transfer. For example, Tsinghua Unigroup's attempted but failed minority investment into U.S. hard drive maker Western Digital is another case where Beijing had attempted to end-run CFIUS with creative investment structures,[2] as was the failed attempt by Canyon Bridge, an acquisition proxy of the Chinese State Council, to purchase Lattice Semiconductor.[3] These are the examples where CFIUS worked, and yet unfortunately, the number of examples where China has successfully avoided U.S. regulatory regimes to prevent technology transfer harmful U.S. national security are increasing. The Chinese are learning our system, identifying its gaps and weaknesses, and finding new ways to exploit American technology to their advantage.

More importantly, these activities have a direct and lasting negative impact on U.S. national security. As the Communist Party seeks to enhance all aspects of its national comprehensive

---

[1] William Hannas, James Mulvenon, and Anna Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization*, London: Routledge, May 2013.
[2] Joshua Jamerson and Eva Dou, "Chinese Firm Ends Investment in Western Digital, Complicating SanDisk Tie-Up," *Wall Street Journal*, 23 February 2016, accessed at: https://www.wsj.com/articles/unispledour-ends-investment-in-western-digital-complicating-sandisk-tie-up-1456231018
[3] Liana Baker, "Trump Bars Chinese-Backed Firm from Buying U.S. Chipmaker Lattice," *Reuters*, 13 September 2017, https://www.reuters.com/article/us-lattice-m-a-canyonbridge-trump/trump-bars-chinese-backed-firm-from-buying-u-s-chipmaker-lattice-idUSKCN1BO2ME

power, U.S. comparative advantages will become all the more important in sustaining U.S. leadership on the battlefield, including in advanced technologies. For example, the Pentagon's "third offset" strategy seeks to leverage current U.S. commercial technological advantages in key areas, such as artificial intelligence and machine learning, to enhance our war fighting capability vis-a-vis China and a resurgent Russia.[4] Yet if our porous investment security and export control regime is not improved, Beijing may be able to turn these current American advantages into their own by investing in, acquiring, or co-opting critical technology. This will allow China to deny the United States' ability to leverage critical technologies for its national security, and further close the gap with the U.S. in areas of key military systems and applications ranging from hypersonic glide vehicles to AI-enabled cyber defense systems.

Although American companies are one of Beijing's highest priority targets in the race to close the technological gap with the United States, the current tech transfer crisis is not entirely their fault. In the China market, American companies confront a comprehensive, state-directed economic and technology development strategy designed to promote technology transfer from foreign multinationals and elevate domestic companies to compete with those multinationals in the global market.[5] This strategy is one personally touted by President Xi Jinping, who declared at a recent Communist Party Meeting that the Chinese state must determine which technologies to develop on its own, which to induce or co-opt from abroad, and which to develop in partnership with Chinese entities.[6] Xi's personal vision has been codified into a more concrete strategy with a number of key overt features:

- Promulgation of state industrial planning documents outlining how Beijing would use its substantial regulatory leverage and financial resources to promote technology transfer and (e.g., "2006-2020 Mid-to-Long Range S&T Plan" and "Made in China 2025"[7])
- Implementation of the strategy of "military-civilian fusion" that expands "civil-military integration" of defense and civilian industrial bases to facilitate the "construction of a national infrastructure that connects the PLA, state-owned defense research, development, and manufacturing enterprises, government agencies under the State Council, universities, and private sector firms."[8]

---

[4] https://www.defense.gov/News/Article/Article/991434/deputy-secretary-third-offset-strategy-bolsters-americas-military-deterrence/

[5] For an overview, see Jane Perlez, Paul Mozur And Jonathan Ansfield, "China's Technology Ambitions Could Upset the Global Trade Order," *New York Times*, 7 November 2017, accessed at:
https://www.nytimes.com/2017/11/07/business/made-in-china-technology-trade.html?_r=0

[6] https://chinacopyrightandmedia.wordpress.com/2016/04/19/xi-jinping-gives-speech-at-cybersecurity-and-informatization-work-conference/

[7] See U.S. Chamber of Commerce, *Made in China 2025: Global Ambitions Built on Local Protections*, 2017, accessed at:
https://www.uschamber.com/sites/default/files/final_made_in_china_2025_report_full.pdf

[8] Greg Levesque and Mark Stokes, *Blurred Lines: Military-Civil Fusion and the "Going Out" of China's Defense Industry*, Pointe Bello, December 2016, accessed at:
https://static1.squarespace.com/static/569925bfe0327c837e2e9a94/t/593dad0320099e64e1ca92a5/1497214574912/062017_Pointe+Bello_Military+Civil+Fusion+Report.pdf

- Provision of massive state subsidies (e.g., IC Fund) to benefit Chinese companies, often masked in ways to skirt WTO prohibitions (according to the U.S Chamber's analysis of Made in China 2025, China will "provide preferential access to capital to domestic companies in order to promote their indigenous research and development capabilities, *support their ability to acquire technology from abroad*, and enhance their overall competitiveness"[9]). Other benefits include "fiscal stimulus, tax reductions and holidays, access to low-cost or free land, low-interest credit, easier access to securities markets, patent approvals, discriminatory technical standards, antitrust policy directed against disfavored competitors, privileged government procurement, limits on market access, and other preferential policies."[10]
- Promotion of "national champion" companies (e.g., Huawei) to supplant multinational companies in the China market and globally[11]
- Promulgation of laws and regulations codifying asymmetries in playing field for U.S. companies operating in China using a very broad definition for what constitutes national security (e.g., Anti-Monopoly Law,[12] Cybersecurity Law,[13] Counter-Espionage Law,[14] National Security Law,[15] Counter-Terrorism Law[16])
- The use of a domestic standards regime, especially with respect to information communication and telecommunications, as a trade weapon to advantage Chinese companies (e.g., WAPI, draft China CPU/OS/computer standards, and the 5G cellular standard)[17]

---

[9] See U.S. Chamber of Commerce, *Made in China 2025: Global Ambitions Built on Local Protections*, 2017, accessed at: https://www.uschamber.com/sites/default/files/final_made_in_china_2025_report_full.pdf

[10] Scott Kennedy, "Evaluating CFIUS: Challenges Posed by a Changing Global Economy," Statement Before the House Committee on Financial Services, Subcommittee on Monetary Policy and Trade, 9 January 2018, accessed at: https://financialservices.house.gov/uploadedfiles/hhrg-115-ba19-wstate-skennedy-20180109.pdf

[11] James McGregor, *China's Drive for 'Indigenous Innovation: A Web of Industrial Policies*, Washington, DC: US Chamber of Commerce, July 2010.

[12] U.S. Chamber of Commerce, *Competing Interests in China's Competition Law Enforcement: China's Anti-Monopoly Law Application and the Role of Industrial Policy*, accessed at: https://www.uschamber.com/sites/default/files/aml_final_090814_final_locked.pdf

[13] https://www.chinalawtranslate.com/cybersecuritylaw/?lang=en

[14] https://www.chinalawtranslate.com/anti-espionage/?lang=en

[15] http://www.chinalawtranslate.com/2015nsl/?lang=en

[16] https://www.chinalawtranslate.com/%E5%8F%8D%E6%81%90%E6%80%96%E4%B8%BB%E4%B9%89%E6%B3%95-%EF%BC%882015%EF%BC%89/?lang=en

[17] Dan Breznitz and Michael Murphree, "The Rise of China in Technology Standards: New Norms in Old Institutions," report prepared for the U.S.-China Economic and Security Review Commission, 16 January 2013, accessed at: https://www.uscc.gov/sites/default/files/Research/RiseofChinainTechnologyStandards.pdf

- Promotion of "buy local" laws to disadvantage foreign firms, especially in information and communications technologies[18]
- Strategies to attract priority foreign investment in China, especially joint ventures and "greenfield" investments[19]
- Mercantilist investment structures globally designed to create infrastructure path dependencies for Chinese state-owned enterprises ("One Belt, One Road")[20] and quasi private companies that China aims to ensure will provide the hardware and software that will underpin all critical infrastructure of the future, from power grids to telecom networks to e-payments infrastructure.

And some covert, illicit features:

- Beijing's well-documented, planetary-scale, government-directed cyber espionage program[21]
- Large-scale, government-directed technology espionage[22]

---

[18] U.S. Chamber of Commerce, *Preventing Deglobalization: An Economic and Security Argument for Free Trade and Investment in ICT*, 2016, accessed at: https://www.uschamber.com/sites/default/files/documents/files/preventing_deglobalization_1.pdf

[19] For the best data on the subject, see the American Enterprise Institute's China Global Investment Tracker at https://www.aei.org/china-global-investment-tracker/ and The Rhodium Group's China Investment Monitor at http://rhg.com/interactive/china-investment-monitor

[20] Christopher Johnson, *President Xi Jinping's "Belt and Road" Initiative: A Practical Assessment of the Chinese Communist Party's Roadmap for China's Global Resurgence,* Center for Strategic and International Studies, March 2016, accessed at: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/160328_Johnson_PresidentXiJinping_Web.pdf

[21] See *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*, Office of the National Counterintelligence Executive, October 2011, at https://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf; ThreatConnect, *CameraShy: Closing the Aperture on China's Unit 78020*, at https://www.threatconnect.com/camerashy/; Mandiant, *APT1: Exposing One of China's Cyber Espionage Units*, accessed at: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf; Dmitri Alperovitch, *Revealed: Operation Shady RAT*, McAfee, August 2011; McAfee® Foundstone® Professional Services and McAfee Labs, Global Energy Cyberattacks: 'Night Dragon', 10 February 2011, accessed at: http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf; Bryan Krekel, Patton Adams, and George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, (report prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman Corp), March 7, 2012; and *Operation SMN: Axiom Threat Actor Group Report*, accessed at: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

[22] Peter Mattis, "Testimony before the U.S.-China Economic and Security Review Commission: Chinese Human Intelligence Operations against the United States," 2 June 2016,

- Non-traditional collection (e.g., the "1000 Talents Program")[23]
- New types of hybrid cyber and human technology espionage (According to the 2016 U.S-China Economic and Security Review Commission report: "China appears to be conducting a campaign of commercial espionage against U.S. companies involving a combination of cyber espionage and human infiltration to systematically penetrate the information systems of U.S. companies to steal their intellectual property, devalue them, and acquire them at dramatically reduced prices."[24])

Any one of these strategies or policies in isolation would be problematic for the U.S. government and American companies, but their simultaneous and often coordinated implementation with the explicit support of PRC government leadership presents an unprecedented challenge.

Categories of Concern

Unfortunately, there are numerous public examples of the significant failures of the current U.S. legal and regulatory system in preventing the loss of critical technology to China. In part, these losses are due to ownership changes in critical American companies through both inbound Chinese investment and outbound U.S. investment to China, which potentially cause harm to U.S. national security.

Beijing's efforts to acquire advanced semiconductor technology such as microprocessors, or the brains of modern electronics, is a sobering example of these failures. Faced with CFIUS' likely blocking of any attempt to buy outright a U.S. microprocessor firm, Beijing has exploited loopholes in both CFIUS and the export control regime to successfully acquire some of these critical technologies. China's goals in acquiring American microprocessor technology are two-fold: (1) subvert current U.S. export controls that prohibit the sale of such advanced chips to be installed in Chinese supercomputers[25] by acquiring the underlying technology and know-how necessary to reproduce the chips indigenously in China, and (2) over the long-term, reduce reliance on American suppliers by fostering a viable and globally competitive domestic industry. Examples of advanced U.S. semiconductor technologies acquired by China in ways that appear to avoid both CFIUS and export controls include:

- *IBM Power8 High-Performance Microprocessor Architecture Technology:* IBM's decided to license elements of the 22nm Power8 high performance server and supercomputer chip architecture to Chinese partners with extensive commercial

---

accessed at:
http://www.uscc.gov/sites/default/files/Peter%20Mattis_Written%20Testimony060916.pdf

[23] William Hannas, James Mulvenon, and Anna Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization*, London: Routledge, May 2013.

[24] *USCC 2016 Annual Report*, accessed at:
https://www.uscc.gov/sites/default/files/annual_reports/2016%20Annual%20Report%20to%20Congress.pdf

[25] https://www.theregister.co.uk/2015/04/10/us_intel_china_ban/

relationships with the PRC government.[26] This is the later generation of a chip architecture that previously received hundreds of millions in development funds from DARPA,[27] and is currently deployed in systems to maintain our nuclear arsenal.[28]

- *AMD High-Performance X86 Microprocessor Technology:* AMD licensed its high performance x86 microprocessor design architecture and transfered the necessary know-how needed to replicate this chip to a consortia of shadowy Chinese companies performing supercomputing work for the Chinese military and defense-industrial base.[29] Through the AMD deal, the Chinese government acquired both a back-door to Intel's technology, since much of AMD's and Intel IP is co-shared, and also created potential vulnerabilities in U.S. weapons systems, many of which use x86-based computing systems.[30] Ironically, while AMD assists the Chinese Government in the development of its supercomputers, it is also receiving millions in U.S. taxpayer dollars to develop similar technologies for the U.S. Department of Energy's next generation supercomputer.[31]
- *Qualcomm Advanced 10nm Server Chip Processor Technology:* Qualcomm's Chinese government subsidized joint venture Huaxintong Semiconductor[32] is working to develop high-end server chips based on the worlds most advanced 10nm process node technology.[33]

Other examples outside of the semiconductor space include Microsoft's joint venture with China's defense electronics conglomerate China Electronic Technology Group Corporation,[34]

---

[26] Paul Mozur, "IBM Venture with China Stirs Concerns," *New York Times*, 19 April 2015, accessed at: https://www.nytimes.com/2015/04/20/business/ibm-project-in-china-raises-us-concerns.html.

[27] https://www-03.ibm.com/press/us/en/pressrelease/20671.wss

[28] The beta of Department of Energy's "Sierra" supercomputer is based on the Power 8 chip, and used for nuclear weapons arsenal stewardship. https://computation.llnl.gov/computers/sierra. The final version will be based on the Power9 chip.

[29] Don Clark, "AMD to License Chip Technology to China Chip Venture," *Wall Street Journal*, 21 April 2016, accessed at: https://www.wsj.com/articles/amd-to-license-chip-technology-to-china-chip-venture-1461269701; Jane Perlez, Paul Mozer and Jonathan Ansfield, "China's Technology Ambitions Could Upset the Global Trade Order," *New York* Times, 7 November 2017, accessed at: https://www.nytimes.com/2017/11/07/business/made-in-china-technology-trade.html.

[30]

[31] http://www.amd.com/en-us/press-releases/Pages/amd-selected-by-2017jun15.aspx

[32] David Barboza, "How This Tech Giant is Backing China's Tech Ambitions," *New York* Times, 4 August 2017, accessed at: https://www.nytimes.com/2017/08/04/technology/qualcomm-china-trump-tech-trade.html?mtrref=undefined&gwh=3307243E0E2CB283EF310DDBEBEB2C50&gwt=pay

[33] https://www.qualcomm.com/news/onq/2017/11/08/qa-anand-chandrasekher-discusses-qualcomm-centriq-2400

[34] Gregg Keizer, "Microsoft Partners with Chinese State-Owned Defense Conglomerate to Promote, Sell Windows 10 to Government," *ComputerWorld*, 18 December 2015, accessed at:

which has five numbered institutes on the Department of Commerce's denied entity list for export control violations;[35] and Chinese investment in artificial intelligence company Neurala.[36] Again, in nearly all of these examples, CFIUS did not appear to have jurisdiction over the transaction, nor did export controls effectively limit the loss of critical know-how and IP flowing to Chinese state entities.

Why FIRRMA is Needed

Passage of the proposed Foreign Investment Risk Review Modernization Act (FIRRMA), S.2098, would constitute a significant step in the right direction to reform CFIUS to deal with these new and evolving approaches inherent in China's strategy. FIRRMA offers essential new tools to ensure future transactions:

- Monitors transactions, transfers, agreements, or arrangements designed to evade or circumvent CFIUS and U.S. export controls
- Expands the scope of review to include real estate transactions near sensitive U.S facilities
- Widens the scope of review to include joint ventures and minority-position investments that are "non-controlling" but "non-passive," with the goal of preventing investment-driven transfers of technology or technology "contributions" by the U.S. partner, and also monitors changes in foreign investors' rights, especially increases in ownership percentage after approvals.
- Broadens CFIUS' definition of "critical technologies" to include emerging technologies such as artificial intelligence, robotics, and machine learning that could strengthen another country's military technologies
- Mandates review of transactions in which the foreign entity is more than 25% owned by a foreign government, which is particularly important with Chinese state-owned enterprises[37]

---

https://www.computerworld.com/article/3016921/microsoft-windows/microsoft-partners-with-chinese-state-owned-defense-conglomerate-to-promote-sell-windows-10-to-gove.html

[35] https://www.bis.doc.gov/index.php/forms-documents/regulations-docs/federal-register-notices/federal-register-2014/957-744-supp-4-1/file.

[36] Jonathan Ray, Katie Atha, Edward Francis, Caleb Dependahl, James Mulvenon, Daniel Alderman, and Leigh Ann Ragland-Luce, *China's Industrial and Military Robotics Development*, Research Report Prepared on Behalf of the U.S.-China Economic and Security Review Commission, October 2016, accessed at: https://www.uscc.gov/sites/default/files/Research/DGI_China%27s%20Industrial%20and%20Military%20Robotics%20Development.pdf

[37] While Chinese state-owned enterprises are perennial source of concern, one must not fall into the trap of thinking that private Chinese companies do not participate in state-sponsored technology theft and espionage. Recently, Derek Scissors from the American Enterprise Institute gave the following testimony to the House Financial Services Subcommittee:

"More important, there is no difference in the control the Communist Party can exercise over private firms and SOEs. There is no rule of law in the PRC, no court or media through which

- Changes evaluation criteria to include "whether the transaction involves a country of special concern that has a demonstrated or declared the strategic goal of acquiring a type of critical technology that a U.S. business that is a party to the transaction possesses"
- Adds badly needed new evaluation factors, including cybersecurity threats and protection of personally identifiable information (PII), etc.

These changes would modernize the CFIUS system to keep pace with the changes in China's strategy and its coordinated national technology policies described above, as well as make the process nimble and flexible enough to adapt to future changes in methods.

Notwithstanding assertions that FIRRMA would duplicate export controls, the reality is wildly different. In fact, FIRRMA includes a critical deferral to U.S. export controls, which all agree constitute the first line of defense to protect U.S. national security concerns. This deferral would prevent duplicative reviews and unnecessary burdens on U.S. companies. Thus, to the extent current U.S. export controls are improved in the future, those improvements would reduce the number of transactions subject to CFIUS jurisdiction under FIRRMA. Moreover, CFIUS and the Bureau of Industry and Security, which administers U.S. export controls, have long engaged regularly in the context of CFIUS reviews. The reality is that CFIUS and U.S. export controls are complimentary and do not and should not operate in exclusive domains going forward.

Why U.S. Export Controls Are Not Enough

A common criticism of FIRRMA is that it seeks to expand CFIUS to cover activities already adequately addressed by the current export control system. Yet the export control system has a number of key flaws:

- First, export controls are product and even feature specific and therefore inherently narrow. With enough financial motivation, some U.S. companies may "design-out" or "de-architect" specific aspects of the technology being transferred that would otherwise trigger export controls. This approach is akin to providing China with 70 percent of the latest technology, with China then being able to use its massive financial resources, overseas investment acquisition campaign, and state-sponsored commercial espionage apparatus to quickly close the remaining 30 percent gap. The upshot is that such ventures greatly accelerate the pace of China's ability to master critical technologies that are of vital concern to U.S. national security.
- Second, once a joint venture is launched in China with a controlled technology, engineers of the U.S. company may then come under intense pressure to assist the Chinese partner to address limitations of the controlled technology. This is akin to your auto dealer

---

private Chinese firms can resist Party orders to ignore US law or steal technology. Private Chinese companies receive less in the way of subsidies but are as beholden to the Party for their survival as SOEs are. There is no justification to treat them differently with regard to national security."

https://financialservices.house.gov/uploadedfiles/hhrg-115-ba19-wstate-dscissors-20180109.pdf

putting a speed limiter on a sports car, only for it to be removed easily in the owner's home garage under duress. In short, it is highly unrealistic—even foolhardy—to expect export controls, including deemed exports, to be able to effectively protect against certain transfers of "know-how" from individual engineers or subject matter experts operating inside of a joint venture on Chinese soil. This is particularly the case as one considers the pressures on engineers employed by U.S. companies operating in China given the objectives and actions of the CCP and under increasingly intense CCP control under Xi Jinping.

- Third, the system is not nimble or quick enough to include rapidly emerging, dual-use technologies that could have significant military implications
- Fourth, because the current structure focuses on technology controls rather than transactions, it does not protect adequately against leakage through supply chains or intra-company transfers after ownership or equity changes or combinations into joint ventures.

Moreover, the export control system has been proven to be largely ineffective at identifying proper "risk of diversion" to military entities once the technology has been transferred to China. For example, despite the glaringly obvious risks, export licenses were granted to UTC to sell its military-grade attack helicopter control software to Chinese defense companies.[38] For its part, Intel was initially permitted but later blocked from selling chips to the developers of Chinese military supercomputers.[39] While the U.S. Government took enforcement actions to rectify both of these situations, in both cases it was too late - the technology had already been transferred to China and was key to enhancing Chinese capabilities. The Commerce Department list of denied export entities is also not updated to reflect CFIUS actions – for example, San'an optoelectronics,[40] a Chinese chip firm twice blocked by CFIUS in an attempt to acquire military technology, is still not on the denied entities list, and American firms continue selling sensitive technology to Sanan' directly.[41]

Conclusion

The Chinese government's economic development and technology modernization strategies and policies have created a sub-optimal business environment for U.S. companies in China and presented new challenges to the investment approval, counter-espionage, and export control efforts of the U.S. Government. Passage of FIRRMA in its current form would be a critical step forward in evolving those efforts to protect U.S. national security while still promoting and supporting foreign investment in the U.S. and the ability of U.S. companies to innovate and grow in the China market and globally.

---

[38] https://www.justice.gov/opa/pr/united-technologies-subsidiary-pleads-guilty-criminal-charges-helping-china-develop-new

[39] https://www.theregister.co.uk/2015/04/10/us_intel_china_ban/

[40] https://www.ledinside.com/news/2016/8/gcs_holdings_sell_to_sanan_opto_blocked_by_us_authorities_to_form_joint_venture and https://www.wsj.com/articles/u-s-regulators-move-to-stop-chinese-takeover-of-german-tech-firm-aixtron-1479549362

[41] https://about.keysight.com/en/newsroom/pr/2016/22apr-nrb16060.shtml?cc=FR&lc=fre

While I share the concerns of some that a significant expansion in the scope of CFIUS review must be matched by a commensurate increase in resources, especially additional qualified personnel. the U.S. Congress has always ensured that our national security comes first and ensured adequate funding to ensure technology supremacy on the battlefield and safeguard the homeland. Make no mistake, China's industrial policies, including China's outbound investment campaign and inbound investment coercive tactics designed to acquire technologies that are critical to U.S. national security, represent an exigent threat in both areas, and China is closing any remaining gaps rapidly. It is essential that the Congress work closely with the Administration to ensure that CFIUS is adequately resourced to address this clear and present threat, while ensuring that our CFIUS system operates efficiently and allows the foreign direct investment that is important to driving growth and creating jobs at home.

RESPONSES TO WRITTEN QUESTIONS OF CHAIRMAN CRAPO FROM CHRISTOPHER PADILLA

Q.1. Your written testimony expresses support for specific provisions of the bill and concerns about specific provisions.

Please discuss the one critical provision of the bill that is essential to CFIUS' protection of national security, and the one provision that you feel most needs further amendment to improve the bill.

A.1. There are several gaps in the current authority of CFIUS that FIRRMA would effectively address. One such gap in the authority of the Committee to assess foreign investments in the United States for national security risks is real estate transactions near military bases or other sensitive Government facilities. FIRRMA appropriately fills this gap. In addition, the bill would give CFIUS expanded authority over certain inbound transactions that are less than controlling, but more than passive. Depending on the circumstances of such a noncontrolling, nonpassive investment, there may be national security issues posed that CFIUS should have the authority to address, and FIRRMA provides that.

Conversely, Sec. 3(B)(v) of FIRRMA significantly expands the definition of "covered transaction," giving CFIUS jurisdiction over outbound and overseas transactions. CFIUS should not govern, nor was it established to review, outbound transactions. This provision should be removed and amended with new language to appropriately reflect the need to enforce and update existing export control regulations to address relevant national security concerns in outbound and overseas transactions. The appropriate U.S. Government agencies that administer export controls should work closely with industry to identify and target critical technology controls, including updating lists of militarily critical technologies that should be considered for control.

Q.2. Much of the concern surrounding this reform effort is about China acquiring cutting edge technology by stealing, reverse engineering, or investing in companies that develop the technology.

Is there a way for emergent "critical" technologies to be appropriately defined and applied by CFIUS?

A.2. Export control agencies have the technical expertise and established industry advisory groups to identify emergent critical technologies. Indeed, in the Export Administration Act, Congress mandated that the Department of Defense, in consultation with other agencies, should maintain a list of military critical technologies and update it to reflect technological advances. From that list, specific export controls and technology transfer limits would be drawn. But the MCTL has fallen into disuse.

Rather than re-create the process in CFIUS, which lacks the expertise to perform this mission, technical experts in the export control agencies (including the Defense Department) are best situated

to make such an assessment. If improvements are needed in this process, then Congress should ensure that the export control agencies have the necessary resources, direction and focus to accomplish this task. Since new technologies are created continually, it is important that the effort to identify emergent critical technologies be ongoing and conducted with input from industry as well as academic experts. Ideally, technologies identified as requiring control would also be discussed with U.S. allies, to develop effective technology controls that are effective and internationally consistent.

Q.2.a. Given the claim that China is acquiring the technology through various means, is reforming solely CFIUS statute and regulations the best way to solve the problem?

A.2.a. No. As cited in my written testimony to the Committee, there are several ways in which CFIUS could be reformed through FIRRMA to address increased national security threats from certain inbound investment transactions.

However, reform of and application of CFIUS alone is not the answer. There is existing authority in export control regulations to govern the transfer of technology to a foreign person, regardless of the type of transaction. Where appropriate, we should use existing export control regimes to identify, define, and control emerging technologies to prevent transfers of technology that could create a national security threat to the United States. Moreover, restricting access to U.S. technologies on a strictly unilateral basis, whether via export controls or CFIUS, will not ensure that the United States maintains its technological lead. Other countries are investing heavily in the development of new technologies, and the United States must seek an internationally effective export control regime, as well as increasing its own investments in research and development across a broad range of technologies to ensure that it will not be overtaken in the race for technological supremacy.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR COTTON FROM CHRISTOPHER PADILLA

Q.1. What other collaborative arrangements, including joint ventures, does IBM currently have in China with Chinese companies, and was CFIUS able to review those for risks to U.S. national security?

A.1. All IBM technology partnerships in China are reviewed against the U.S. Government's lists of restricted end-users and activities, including military end-users and proliferation screening. Additionally, our agreements mandate that all partner companies also comply with U.S. export control regulations, including restrictions on military end use. IBM's activities in China comply with U.S. law and export control regulations, and, where necessary, have received approval from the necessary export licensing agencies. In addition, IBM has been through two CFIUS reviews for business transactions with Chinese companies, both of which were subject to a rigorous review and to risk mitigation agreements with appropriate U.S. Government agencies.

Q.2. What such arrangements do you have planned for the near future, and is CFIUS able to review any of those for risks to U.S. national security?

A.2. While we cannot speculate on future business decisions, IBM believes that under existing CFIUS regulations and export control regulations, there is ample authority to govern and vet transactions for risks to national security. As mentioned in my testimony, IBM supports both the expansion of CFIUS jurisdiction over certain inbound investment transactions, as well as an updated and comprehensive review of militarily critical technologies that should be controlled for export from the United States.

Q.2.a. What dual-use technology and know-how has IBM transferred to China over the last decade, and what impact do you think that has had on the United States' relative technological advantage in areas of national security?

A.2.a. Most IBM business transactions in China do not require an individual export license for either goods or technology, but in every transaction there is an obligation to comply with U.S. Export Administration Regulations as well as other relevant provisions of U.S. law. IBM business in China is fully compliant with U.S. law and export regulations. It should be noted that as a general matter of policy, U.S. export controls have long limited the transfer of technology to China to levels that are several generations behind current, cutting-edge technologies sold in other markets.

Q.3. Over the past 10 years or so, has IBM been pressured by Chinese entities to turn over valuable technology and know-how to Chinese companies? If so, what types?

A.3. No. Our business decisions in China are driven by commercial considerations and by the limits established in U.S. export control laws and regulations.

Q.4. Has IBM been pressured by Chinese entities to oppose, criticize, or help defeat the Foreign Investment Risk Review Modernization Act?

A.4. No. Even if we had been asked to do so, IBM would have refused. Our position on this legislation is not driven by pressure from foreign governments, but rather from our long experience in international markets and direct experience with both CFIUS reviews and U.S. export control laws.

Q.5. When U.S. companies engage in activities on Chinese soil that could negatively impact the United States' national security, do you believe the Federal Government has a legitimate interest in being notified and afforded a chance to assess the risks for U.S. national security?

A.5. Yes. This is why the United States has a robust and multilateral export control system to review, assess, and mitigate legitimate risks to U.S. national security in commercial transactions overseas.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR MENENDEZ FROM CHRISTOPHER PADILLA

Q.1. The legislation introduced by Senators Cornyn and Feinstein would add five new types of covered transactions to CFIUS' purview and it would expand the definition of "critical technologies."

Q.1.a. Can you comment on whether CFIUS and its member agencies currently have sufficient resources to monitor foreign investment and acquisitions, review filed transactions, and conduct thorough reviews and investigations in the required time periods?

A.1.a. There is a time lag in CFIUS' issuance of public data about its work, but the available data indicate that there has been a material rise in the number of investigations conducted by CFIUS, which places stress on CFIUS resources. Substantially increasing the CFIUS workload, as we believe FIRRMA would do, would exacerbate this stress.

Q.1.b. In your opinion, should any expansion of authority also include new resources, funding, and staffing for the panel?

A.1.b. Yes. We agree with providing badly needed resources to the Committee. The CFIUS case load has increased significantly in recent years, and staff resources are already stretched thin. Even if Congress does not elect to give CFIUS an expanded mandate, it should provide additional resources for CFIUS to do its job and manage the existing case load effectively.

Q.2. Last year, Ness Technologies, a New Jersey-based software engineering company, had agreed to be purchased by HNA, a Chinese conglomerate, on the condition that the transaction received approval from CFIUS. According to a lawsuit filed by Ness Technologies last month, that deal fell apart because HNA provided "knowingly false, inconsistent, and misleading information" about its ownership and ties to the Chinese government during CFIUS' review of the acquisition. HNA's interests in the United States are certainly not limited to Ness Technologies—they've received CFIUS approval to purchase a California technology distributor and they are actively working to purchase a controlling stake in SkyBridge Capital, the investment firm owned by Anthony Scaramucci. This case raises important questions about the consequences of failing to provide accurate information or knowingly providing false information to CFIUS.

Q.2.a. What steps should CFIUS take, if any, with regard to other transactions, either previously approved or pending approval, involving a party if CFIUS determines that party has misled the panel. For example, should the panel reopen previously cleared HNA transactions or modify their approach to reviewing pending transactions in light of this information?

A.2.a. IBM cannot comment on the HNA transaction or other specific transactions in which IBM is not a party. However, generally speaking, IBM believes that it would be fully appropriate for CFIUS to reopen a review or investigation of a transaction if new evidence comes to light indicating that one or more of the parties provided false or misleading information during the CFIUS process. IBM believes that CFIUS currently has the authority to do so and supports efforts to further clarify this authority in FIRRMA.

Q.2.b. What should be the consequences of a party misleading or failing to provide accurate information to CFIUS?

A.2.b. Transaction denial and unwinding of previously approved transactions are the current remedies. These remedies are severe but appropriate in a situation involving the provision of false or misleading information.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR WARNER FROM CHRISTOPHER PADILLA

Q.1. As we search for the most appropriate remedy to the very real problem of foreign countries gaining access to critical U.S. technologies, I've heard some suggest that we should be pursuing other changes instead of or in addition to the Committee on Foreign Investment in the United States (CFIUS) reform.

Q.1.a. What role should export controls play in addressing this problem?

Could the export control system be modified to address the concern that know how—not just intellectual property (IP)—is being transferred through joint ventures (JVs) and other partnerships?

A.1.a. Existing U.S. export controls already address the issue of the transfer of "know how," and they have done so for several decades. No modification to the export control system is necessary to address this concern. IBM believes that the real issue here is that the lists of controlled technology (which includes know how) have not kept pace with technological advances. The solution is for Congress to exercise its oversight authority to ensure that the U.S. export control agencies update their control lists so that they cover know how of concern from a national security perspective. The U.S. export control agencies already have the authority to make such updates immediately—they do not have to wait for the multilateral system to agree in order to do so.

Q.1.b. Are there other fixes outside of CFIUS that should be considered to address this security challenge?

A.1.b. The U.S. Export Administration Regulations (EAR) currently provide a mechanism to address concerns about access to emerging U.S. technologies. These regulations can already control for export emerging technologies that are dual-use (*i.e.,* have both commercial and military applications) and that have potential national security implications. Specifically, 15 C.F.R. § 742.6(a)(7) establishes a mechanism for the Commerce Department, with concurrence from the Defense and State Departments, to designate for control items that are not currently covered by the multilateral export control regime (Wassenaar Arrangement) but nonetheless "should be controlled for export because the items provide at least a significant military or intelligence advantage to the United States or for foreign policy reasons . . . ". Items designated under this unilateral export control mechanism (denoted by classification in the ECCN 0Y521 series) are controlled for export—and thus require an export license issued by the Commerce Department—to all countries except Canada (subject to limited exception). These items are temporarily controlled for export for one calendar year (subject to limited extension), providing time for the Commerce Department

to transition the items to a more permanent control status. Such a transition may occur upon an item's incorporation into the multilateral export control regime, or it may occur upon a determination by the Commerce Department that a more permanent unilateral control is appropriate. The Commerce Department also has the option to de-control an item, if warranted. Four categories of items (including related technology) have been controlled for export in this manner since creation of the unilateral export control mechanism in 2012. Publicly available data indicate that eight licenses were issued with respect to such items in 2015.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR CORTEZ MASTO FROM CHRISTOPHER PADILLA

Gaming and Tourism

Q.1. Foreign companies are beginning to expand into new industries, including gaming and tourism in the State of Nevada. As an example, foreign companies have been investing in and developing properties on the Las Vegas Strip. In the context of CFIUS reviews, hotel deals previously examined by the committee include the acquisition of New York's Waldorf-Astoria Hotel by Anbang Insurance Group in 2014.

Q.1.a. Given the importance of the tourism industry to Nevada, could you elaborate on the concerns associated with foreign acquisition of hotels or tourism companies in the United States?

A.1.a. To the extent that the acquisition of hotels or tourism companies present a national security risk, CFIUS already has authority to review such transactions. As an information technology solutions company, I regret that IBM has no basis on which to comment further on any concerns that might exist within the hotel and tourism industry.

Q.1.b. How does CFIUS review such transactions, and what is the Committee's track record on approving or denying these types of deals?

A.1.b. To the extent that the acquisition of hotels or tourism companies present a national security risk, CFIUS already has authority to review such transactions. However, IBM has no particular knowledge of the Committee's track record in reviewing such cases.

CFIUS, Mining and Proximity to Military Installations

Q.2. In the last decade, CFIUS blocked three proposed investments in Nevada mining companies, citing national security concerns regarding the properties' proximity to Fallon Naval Air Station.

How does CFIUS traditionally review such acquisitions as it relates to their location relative to military installations? Is that process working effectively, or are there any areas needed for improvement?

A.2. CFIUS currently has authority to review transactions that include real estate near military or other sensitive facilities when the transaction involves the acquisition of a U.S. business. However, current CFIUS authority does not extend to real estate transactions that include only undeveloped land and are not part of an

acquisition of a U.S. business. As I stated in my testimony, IBM supports the expansion of CFIUS to include such real estate transactions.

Greenfield Acquisition

Q.3. In Nevada, we are home to a number of technology startups, including drone technology.

Can you discuss the potential positive and negative consequences of expanding CFIUS review to "greenfield" projects—or those involving startups?

A.3. Foreign investment in "greenfield projects," in which a foreign entity creates a totally new business in the United States from the ground up, generally represents a positive contribution to the U.S. economy, creating new jobs and boosting economic growth. To the extent that such new businesses are located in proximity to military installations or other sensitive facilities, expansion of CFIUS to cover pure real estate transactions would enable the Committee to address this concern.

In the case of acquisitions or investments that result in foreign control of existing U.S. startup companies, CFIUS already has authority to review such transactions for national security risks, just as it has existing authority to review transactions that result in foreign control of any other U.S. business.

RESPONSES TO WRITTEN QUESTIONS OF CHAIRMAN CRAPO FROM SCOTT KUPOR

Q.1. Your written testimony expresses support for specific provisions of the bill and concerns about specific provisions.

Please discuss the one critical provision of the bill that is essential to CFIUS' protection of national security, and the one provision that you feel most needs further amendment to improve the bill.

A.1. I support modernizing CFIUS to ensure it is reviewing appropriate transactions that safeguard our national security. However, the area of the Foreign Investment Risk Review Modernization Act (FIRRMA) most in need of improvement is clarity that a U.S. venture capital fund with foreign limited partners (*i.e.,* those that invest into a fund, or "LPs") is not implicated. As my testimony details, FIRRMA is currently ambiguous as to whether a U.S. fund or its LPs must file with CFIUS if the fund might invest in critical technologies. FIRRMA should be changed to reflect that neither a U.S. fund nor its foreign LPs need to file with CFIUS when those LPs are passive investors. This means either clarifying that venture funds are outside the scope of the bill entirely, or affirmatively stating that foreign LPs must meet the passive investment test in FIRRMA. If the latter, the passive investment test must be broadened to reflect true passivity. For example, FIRRMA considers an investment to be nonpassive if the investor has access to "any nonpublic technical information in the possession of the United States business" or "any nontechnical information in the possession of the United States business that is not available to all investors." These requirements are too narrow and do not reflect the reality of the marketplace where all shareholders are not subject to the same information at all times. Very early investors—such as angel

investors—may receive less detailed information about a company than other investors, but that is harmless in the vast majority of cases.

Q.2.a. Much of the concern surrounding this reform effort is about China acquiring cutting edge technology by stealing, reverse engineering, or investing in companies that develop the technology.

Is there a way for emergent "critical" technologies to be appropriately defined and applied by CFIUS?

A.2.a. It is imperative that "critical" technologies be specifically defined so the scope of FIRRMA is well understood in the marketplace. Small, high-growth startups are among the most innovative companies in the world. Yet the ability of startups to navigate the regulatory landscape is limited as these companies are resource-constrained. I strongly encourage Congress and CFIUS to keep these small companies in mind as they define critical technology.

I believe Congress should set careful parameters on what critical technology means; otherwise, there will be a temptation by CFIUS to broaden the term out so far as to pull in vast areas of our economy. This will have the effect of potentially slowing down the innovation economy but also taking CFIUS's eye off the areas of technology that could truly impact our national security. To highlight an example, artificial intelligence and machine learning technologies will likely find their way into nearly all companies over the next 5–10 years. We suspect they may be as ubiquitous as core infrastructure elements—such as a database—are today. Thus to legislate at that level of definition will not only curb the development of these critical technologies in the United States, but will also overwhelm the review cycle for CFIUS. Therefore, to the extent Congress seeks to define "critical" technologies, it should do so not only by limiting broad references to foundational technologies, but also by defining the key use cases for which the application of that technology could raise national defense or other core security issues.

Q.2.b. Given the claim that China is acquiring the technology through various means, is reforming solely CFIUS statute and regulations the best way to solve the problem?

A.2.b. Reforming CFIUS is not the sole way to combat technology theft and transfer. The Federal Government can combat technology theft by working closely with the startup, technology, and investor community to identify best practices and communication channels so industries and Government can work together on problem areas. More should be done by law enforcement to train the venture industry and startups on how to combat technology theft and how to garner the attention of law enforcement agencies. Ultimately, if foreign sovereign governments want to steal technology, they are much more likely to do so through formal espionage and theft efforts versus through investing in startup companies. In addition, law enforcement should educate startups on ways to deal with investors that may seek to transfer technology overseas. Finally, the Federal Government should make available more nondilutive capital for startups, whether through the Defense Advanced Research Projects Agency (DARPA), Advanced Research Projects Agency—Energy (ARPA–E), the Small Business Innovation Research (SBIR)

program, or other initiatives. Our industry would be glad to partner with all appropriate Federal agencies on these ideas.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR MENENDEZ FROM SCOTT KUPOR

Q.1. The legislation introduced by Senators Cornyn and Feinstein would add five new types of covered transactions to CFIUS' purview and it would expand the definition of "critical technologies." **Q.1.a.** Can you comment on whether CFIUS and its member agencies currently have sufficient resources to monitor foreign investment and acquisitions, review filed transactions, and conduct thorough reviews and investigations in the required time periods?

A.1.a. I am concerned about the workflow the Foreign Investment Risk Review Modernization Act (FIRRMA) would place on CFIUS if the covered transaction section is not changed to reflect the concerns I raised in my testimony. Specifically, as drafted FIRRMA is unclear on whether a U.S. venture fund with foreign limited partners (*i.e.,* those that invest into a fund, or "LPs") must file with CFIUS, or whether those foreign LPs must file before investing in a fund. LPs do not have access to sensitive information that is the concern of FIRRMA, nor do they have any say in the investment decisions of venture funds. Therefore, FIRRMA should specifically indicate that U.S. venture funds and passive LPs are not covered by the legislation. If this ambiguity is not cleared up venture funds and foreign LPs will very likely file on a precautionary basis with CFIUS because they fear the consequences of not filing when the agency believes a filing was in order. An overabundance of precautionary filings by venture funds and LPs will not improve our national security, and in fact will diminish the benefit of FIRRMA, as CFIUS will be consumed with filings that were never a national security threat in the first place.

Q.1.b. In your opinion, should any expansion of authority also include new resources, funding, and staffing for the panel?

A.1.b. Yes, I believe if CFIUS's mandate is expanded considerably the agency must receive additional resources to ensure it has the ability to be appropriately responsive to the business community. At the same time, I believe Congress should require that CFIUS abide by statutory time lines so the business community understands at the outset when it will receive a decision.

Q.2. Last year, Ness Technologies, a New Jersey-based software engineering company, had agreed to be purchased by HNA, a Chinese conglomerate, on the condition that the transaction received approval from CFIUS. According to a lawsuit filed by Ness Technologies last month, that deal fell apart because HNA provided "knowingly false, inconsistent, and misleading information" about its ownership and ties to the Chinese government during CFIUS' review of the acquisition. HNA's interests in the United States are certainly not limited to Ness Technologies—they've received CFIUS approval to purchase a California technology distributor and they are actively working to purchase a controlling stake in SkyBridge Capital, the investment firm owned by Anthony Scaramucci. This case raises important questions about the consequences of failing

to provide accurate information or knowingly providing false information to CFIUS.

- What steps should CFIUS take, if any, with regard to other transactions, either previously approved or pending approval, involving a party if CFIUS determines that party has misled the panel. For example, should the panel reopen previously cleared HNA transactions or modify their approach to reviewing pending transactions in light of this information?
- What should be the consequences of a party misleading or failing to provide accurate information to CFIUS?

A.2. I appreciate the question, but I am not an expert on CFIUS's current practices or any of its cases. However, I do believe that candor before Government agencies is of the utmost importance.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR WARNER FROM SCOTT KUPOR

Q.1. One of the strengths of the United States is our ability to foster innovation and develop new technologies.

Would the filing times and additional fees associated with CFIUS jurisdiction significantly inhibit venture capital investments and hurt entrepreneurship by creating excessive barriers, such as prolonged wait times, to foreign investment?

A.1. My testimony raised serious concerns about the impact of the Foreign Investment Risk Review Modernization Act (FIRRMA) on U.S. startups and venture capital funds. Presently, FIRRMA is ambiguous as to whether a U.S. venture fund with foreign limited partners (*i.e.,* those that invest into a fund, or "LPs") must file with CFIUS if it might invest in critical technology, or whether the foreign LPs themselves must file with CFIUS. This is despite the fact that LPs are truly passive investors that have no access to sensitive information and no say in investment decisions. If FIRRMA is not clarified to remove U.S. venture funds and their LPs from the scope of the bill, I fear that it will have a lasting impact on foreign investment into venture funds. If foreign LPs must file with CFIUS when they invest in a venture fund—incurring wait times and additional cost in the process—that would be a substantial disincentive to investing in U.S. venture funds. As CFIUS reform proceeds, we must keep in mind that global investors have many choices these days. U.S. startups have seen their share of global venture investment drop from 90 percent 20 years ago, to 81 percent 10 years ago, to 53 percent last year. This means if we make it more burdensome to invest in U.S. startups via U.S. venture funds then we will continue to see a steady decline in our global share, which will further harm our competitiveness.

Q.2. Would significantly expanding CFIUS's jurisdiction negatively affect our investment relationship with Europe and other traditional economic and military allies, who could get caught up in an expansion of CFIUS's scope of review?

A.2. FIRRMA provides that CFIUS may exempt certain counties if the United States has in place a mutual defense treaty with that country and meets other factors. In my testimony, I expressed support for broadening that authority out to a wider group of U.S.

strategic partners. I am concerned that if exemptions are too narrow that FIRRMA will both burden key U.S. allies and inundate CFIUS with filings from countries that are not engaged in the type of activity with which FIRRMA is concerned. I encourage Congress to look at ways to ease burdens imposed on important U.S. allies during the CFIUS process.

Q.3. Do you have a sense of how many increased CFIUS filings a bill like the Foreign Investment Risk Review Modernization Act could result in? Would CFIUS be able to handle the surge in reviews likely to result from a bill like FIRRMA? How much would it need to expand to handle such a caseload?

A.3. A major factor impacting the increase of filings will be whether FIRRMA is improved to clarify that U.S. venture funds nor their LPs must file with CFIUS when those LPs are passive investors in the fund. As my previous answer indicates, unless FIRRMA is modified CFIUS will see many precautionary filings from U.S. venture funds and their foreign LPs that should not be within the scope of the bill. I strongly encourage Congress to narrow the scope of FIRRMA in line with my testimony to ensure CFIUS stays focused on the transactions that truly impact national security. But even if FIRRMA is modified, I believe CFIUS will need additional resources to be responsive to the considerable uptick in filings due to the bill.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR CORTEZ MASTO FROM SCOTT KUPOR

Gaming and Tourism

Q.1. Foreign companies are beginning to expand into new industries, including gaming and tourism in the State of Nevada. As an example, foreign companies have been investing in and developing properties on the Las Vegas Strip. In the context of CFIUS reviews, hotel deals previously examined by the committee include the acquisition of New York's Waldorf-Astoria Hotel by Anbang Insurance Group in 2014.

Q.1.a. Given the importance of the tourism industry to Nevada, could you elaborate on the concerns associated with foreign acquisition of hotels or tourism companies in the United States?

Q.1.b. How does CFIUS review such transactions, and what is the Committee's track record on approving or denying these types of deals?

A.1.a.–b. I appreciate the question, but unfortunately I am not able to answer specifically as the U.S. venture capital industry has had little experience in dealing with gaming-related applications of CFIUS. The reason for this is our industry invests in and partners with startups as they scale and grow, whereas CFIUS's jurisdiction is over transactions where a foreign person is acquiring an existing U.S. entity. My testimony before the Banking Committee pertained to changes the Foreign Investment Risk Review Modernization Act (FIRRMA) proposes for CFIUS that might affect the venture capital industry and startups for the first time. In particular, I am concerned that FIRRMA is unclear on whether a U.S. venture fund

with foreign limited partners (*i.e.,* those that invest into a fund, or "LPs") must file with CFIUS, or whether those foreign LPs must file before investing in a fund. Neither of these options are prudent from a public policy perspective and both would be incredibly disruptive to venture firms. LPs in venture funds have no access to the sensitive information that is the concern of FIRRMA and have no role in the investment decisions of venture funds. Therefore, foreign LPs pose no national security risk to our Nation. But if FIRRMA is not clarified then CFIUS will be confronted with an abundance of precautionary filings from venture firms and their foreign LPs that distract the agency from investments that may pose a national security concern. These precautionary filings will be costly for venture funds and distract investors from partnering with startups to build and scale the company.

CFIUS, Mining and Proximity to Military Installations

Q.2. In the last decade, CFIUS blocked three proposed investments in Nevada mining companies, citing national security concerns regarding the properties' proximity to Fallon Naval Air Station.

How does CFIUS traditionally review such acquisitions as it relates to their location relative to military installations? Is that process working effectively, or are there any areas needed for improvement?

A.2. As previously indicated, I am not an expert on CFIUS as it currently operates and unfortunately unable to answer this question. I would add, however, that focusing CFIUS review on investments in close proximity to military or other sensitive Government installations seems to be a much more appropriate use of CFIUS time than aiming to review passive investments in venture capital funds or venture-backed startups.

Greenfield Acquisition

Q.3. In Nevada, we are home to a number of technology startups, including drone technology.

Can you discuss the potential positive and negative consequences of expanding CFIUS review to "greenfield" projects—or those involving startups?

A.3. Nevada is home to a burgeoning startup ecosystem. From 2013–2017, 190 Nevada startups raised $640 million in venture funding. FIRRMA has the potential to significantly impact startups in Nevada and across the United States. One way startups can be affected is if FIRRMA enables CFIUS to unnecessarily scrutinize U.S. venture capital funds, which partners with many high-growth startups in Nevada. As my written testimony detailed, FIRRMA is ambiguous as to whether a U.S. venture fund with foreign LPs must file with CFIUS. U.S. venture funds have increasingly attracted foreign LPs, which benefits our country because that capital is then invested in U.S. startups. Scrutinizing the LPs of a venture fund is not a good use of CFIUS's time, as these LPs do not have access to sensitive information that is the concern of FIRRMA and have no say in investment decisions of the fund. Our national security would be far better served by focusing on direct investments into U.S. companies where there might be an opportunity for a foreign person to extract sensitive information from a company.

Unless FIRRMA is clarified to remove venture funds from the ambit of the bill, foreign LPs will have a significant disincentive to invest capital in the United States via venture funds. This will in turn harm U.S. startups that need that capital to grow and prosper. Furthermore, the risk capital will simply flow to other non-U.S. startups, compromising not only job growth in the United States, but also making it more likely that long-term hubs of innovation will prosper in markets outside of the United States.

RESPONSES TO WRITTEN QUESTIONS OF CHAIRMAN CRAPO FROM GARY CLYDE HUFBAUER

Q.1. Your written testimony expresses support for specific provisions of the bill and concerns about specific provisions.

Please discuss the one critical provision of the bill that is essential to CFIUS' protection of national security, and the one provision that you feel most needs further amendment to improve the bill.

A.1. The core is the protection of "critical technologies". The legislation should draw on America's best brains—identified by the National Academy of Sciences and the National Academy of Engineering, with assistance from the National Security Agency and the Central Intelligence Agency—to define "critical technologies" for national security purposes. The definitions should be updated at least annually.

Q.2. Much of the concern surrounding this reform effort is about China acquiring cutting edge technology by stealing, reverse engineering, or investing in companies that develop the technology.

Q.2.a. Is there a way for emergent "critical" technologies to be appropriately defined and applied by CFIUS?

A.2.a. The best that can be done for appropriate definition is to rely on the agencies named in my first answer. This should be a central mission of a standing committee of these agencies, with rotating members to obtain expertise on different technologies.

Q.2.b. Given the claim that China is acquiring the technology through various means, is reforming solely CFIUS statute and regulations the best way to solve the problem?

A.2.b. If the CFIUS mandate is enlarged by the pending legislation, it should be closely coordinated with the Export Administration authority. Ideally, the two committees/agencies would be merged, but that may be a step too far. In addition, the CIA's resources and budgets should be expanded to keep abreast with Chinese technology through covert means. It would be worthwhile to ask the GAO for a report on ways to improve civil and criminal prosecution of espionage cases. Over the long term, the only way the United States will maintain technological superiority is through stepped up public and private investment in R&D.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR MENENDEZ FROM GARY CLYDE HUFBAUER

Q.1. The legislation introduced by Senators Cornyn and Feinstein would add five new types of covered transactions to CFIUS' purview and it would expand the definition of "critical technologies."

- Can you comment on whether CFIUS and its member agencies currently have sufficient resources to monitor foreign investment and acquisitions, review filed transactions, and conduct thorough reviews and investigations in the required time periods?
- In your opinion, should any expansion of authority also include new resources, funding, and staffing for the panel?

A.1. In my view, CFIUS resources are hopelessly inadequate for the mandate envisaged by this legislation. Moreover, adequate funds must be provided for the NAS, the NAE, and the intelligence agencies. Unless the Congress is prepared to provide an annual budget in the range of $100 million, the new CFIUS cannot possibly discharge the broader mandate.

Q.2. Last year, Ness Technologies, a New Jersey-based software engineering company, had agreed to be purchased by HNA, a Chinese conglomerate, on the condition that the transaction received approval from CFIUS. According to a lawsuit filed by Ness Technologies last month, that deal fell apart because HNA provided "knowingly false, inconsistent, and misleading information" about its ownership and ties to the Chinese government during CFIUS' review of the acquisition. HNA's interests in the United States are certainly not limited to Ness Technologies—they've received CFIUS approval to purchase a California technology distributor and they are actively working to purchase a controlling stake in SkyBridge Capital, the investment firm owned by Anthony Scaramucci. This case raises important questions about the consequences of failing to provide accurate information or knowingly providing false information to CFIUS.

- What steps should CFIUS take, if any, with regard to other transactions, either previously approved or pending approval, involving a party if CFIUS determines that party has misled the panel? For example, should the panel reopen previously cleared HNA transactions or modify their approach to reviewing pending transactions in light of this information?
- What should be the consequences of a party misleading or failing to provide accurate information to CFIUS?

A.2. When an acquiring company provides "knowingly false" information, it should be disqualified from any new U.S. acquisition for an extended period, say 5 years, and it should be fined quite heavily. But I would not require the company to divest past acquisitions not involving critical technology.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR WARNER FROM GARY CLYDE HUFBAUER

Q.1. Do you think that significantly expanding CFIUS's jurisdiction and identifying "countries of particular concern" for purposes of CFIUS review could be considered a discriminatory measure by trade partners?

What would be the potential consequences of doing so from a trade perspective? Should we expect retaliation? What forms could that retaliation take?

A.1. Yes, this would be regarded as a discriminatory measure, but GATT Article XXI permits discrimination for national security reasons. The target country would not have an actionable complaint in the WTO. But retaliation can certainly be expected, mainly in the form of denied acquisitions by U.S. firms. China and Russia already "wall off" vast sectors of their economies (mainly high-tech) from foreign acquisition, so I suspect that the retaliation would involve other sectors, such as finance, food, education, or health.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR CORTEZ MASTO FROM GARY CLYDE HUFBAUER

Gaming and Tourism

Q.1. Foreign companies are beginning to expand into new industries, including gaming and tourism in the State of Nevada. As an example, foreign companies have been investing in and developing properties on the Las Vegas Strip. In the context of CFIUS reviews, hotel deals previously examined by the committee include the acquisition of New York's Waldorf-Astoria Hotel by Anbang Insurance Group in 2014.

- Given the importance of the tourism industry to Nevada, could you elaborate on the concerns associated with foreign acquisition of hotels or tourism companies in the United States?
- How does CFIUS review such transactions, and what is the Committee's track record on approving or denying these types of deals?

A.1. In my opinion, the acquisition of U.S. hotel and tourism companies by foreign firms, including firms based in adversary nations exemplified by China and Russia, is not a national security concern. While I am not privy to the CFIUS track record on such M&A transactions, I am unaware of any transaction that was blocked.

CFIUS, Mining and Proximity to Military Installations

Q.2. In the last decade, CFIUS blocked three proposed investments in Nevada mining companies, citing national security concerns regarding the properties' proximity to Fallon Naval Air Station.

How does CFIUS traditionally review such acquisitions as it relates to their location relative to military installations? Is that process working effectively, or are there any areas needed for improvement?

A.2. As a rock-hunter in the Fallon area, I know it well. So far as I know, the Pentagon alerts the CFIUS committee when an acquisition is proposed near a military installation. If the Pentagon objects to the acquisition, because of surveillance concerns, I believe the acquisition is routinely denied.

Greenfield Acquisition

Q.3. In Nevada, we are home to a number of technology startups, including drone technology.

Can you discuss the potential positive and negative consequences of expanding CFIUS review to "greenfield" projects—or those involving startups?

A.3. In my view, greenfield projects create much less concern than M&A projects involving the same technology. However, there can be a legitimate worry that the greenfield will hire American personnel with technology expertise. In cases involving critical technology (as identified in my answer to Senator Crapo) it would be appropriate for CFIUS to monitor the personnel employed for a reasonable period (say 5 years). In appropriate cases, surveillance can be authorized by a FISA warrant. In exceptional cases, the foreign firm may be required to divest.

RESPONSES TO WRITTEN QUESTIONS OF CHAIRMAN CRAPO FROM JAMES MULVENON

Q.1. Your written testimony expresses support for specific provisions of the bill and concerns about specific provisions.

Please discuss the one critical provision of the bill that is essential to CFIUS' protection of national security, and the one provision that you feel most needs further amendment to improve the bill.

A.1. Did not respond by publication deadline.

Q.2. Much of the concern surrounding this reform effort is about China acquiring cutting edge technology by stealing, reverse engineering, or investing in companies that develop the technology.

- Is there a way for emergent "critical" technologies to be appropriately defined and applied by CFIUS?
- Given the claim that China is acquiring the technology through various means, is reforming solely CFIUS statute and regulations the best way to solve the problem?

A.2. Did not respond by publication deadline.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR MENENDEZ FROM JAMES MULVENON

Q.1. The legislation introduced by Senators Cornyn and Feinstein would add five new types of covered transactions to CFIUS' purview and it would expand the definition of "critical technologies."

- Can you comment on whether CFIUS and its member agencies currently have sufficient resources to monitor foreign investment and acquisitions, review filed transactions, and conduct thorough reviews and investigations in the required time periods?
- In your opinion, should any expansion of authority also include new resources, funding, and staffing for the panel?

A.1. Did not respond by publication deadline.

Q.2. Last year, Ness Technologies, a New Jersey-based software engineering company, had agreed to be purchased by HNA, a Chinese conglomerate, on the condition that the transaction received approval from CFIUS. According to a lawsuit filed by Ness Technologies last month, that deal fell apart because HNA provided "knowingly false, inconsistent, and misleading information" about its ownership and ties to the Chinese government during CFIUS' review of the acquisition. HNA's interests in the United States are certainly not limited to Ness Technologies—they've received CFIUS

approval to purchase a California technology distributor and they are actively working to purchase a controlling stake in SkyBridge Capital, the investment firm owned by Anthony Scaramucci. This case raises important questions about the consequences of failing to provide accurate information or knowingly providing false information to CFIUS.

- What steps should CFIUS take, if any, with regard to other transactions, either previously approved or pending approval, involving a party if CFIUS determines that party has misled the panel. For example, should the panel reopen previously cleared HNA transactions or modify their approach to reviewing pending transactions in light of this information?
- What should be the consequences of a party misleading or failing to provide accurate information to CFIUS?

A.2. Did not respond by publication deadline.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR WARNER FROM JAMES MULVENON

Q.1. Can you describe how China legally obtains sensitive U.S. technologies through private companies and through joint ventures?

A.1. Did not respond by publication deadline.

Q.2. Many of the technologies that China, Russia, and others are seeking to obtain are at a very early stage, frequently before we know whether there is a military use for them. Many, such as artificial intelligence (AI) and robotics also have far ranging applications that extend well beyond military usage.

How can we encourage investment in these early stage technologies—which is so critical to our U.S. economic dynamism—without giving access to competitor nations and weakening our economic advantage?

A.2. Did not respond by publication deadline.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR CORTEZ MASTO FROM JAMES MULVENON

Gaming and Tourism

Q.1. Foreign companies are beginning to expand into new industries, including gaming and tourism in the State of Nevada. As an example, foreign companies have been investing in and developing properties on the Las Vegas Strip. In the context of CFIUS reviews, hotel deals previously examined by the committee include the acquisition of New York's Waldorf-Astoria Hotel by Anbang Insurance Group in 2014.

- Given the importance of the tourism industry to Nevada, could you elaborate on the concerns associated with foreign acquisition of hotels or tourism companies in the United States?
- How does CFIUS review such transactions, and what is the Committee's track record on approving or denying these types of deals?

A.1. Did not respond by publication deadline.

CFIUS, Mining and Proximity to Military Installations

Q.2. In the last decade, CFIUS blocked three proposed investments in Nevada mining companies, citing national security concerns regarding the properties' proximity to Fallon Naval Air Station.

How does CFIUS traditionally review such acquisitions as it relates to their location relative to military installations? Is that process working effectively, or are there any areas needed for improvement?

A.2. Did not respond by publication deadline.

Greenfield Acquisition

Q.3. In Nevada, we are home to a number of technology startups, including drone technology.

Can you discuss the potential positive and negative consequences of expanding CFIUS review to "greenfield" projects—or those involving startups?

A.3. Did not respond by publication deadline.

FOREIGN INVESTMENT RISK REVIEW MODERNIZATION ACT (FIRRMA)

Bottom Line Up Front. Gaps in the CFIUS process have allowed China to weaponize investment to achieve the back-door transfer of dual-use U.S technology and related know-how, aiding China's military modernization and eventually further shrinking the U.S. defense industrial base. This jeopardizes the ability of the United States to maintain the overall military advantage over potential adversaries that has underpinned our national security and economic prosperity since at least the end of World War II. China is vacuuming up U.S. technology however it can, through both illicit and licit means (e.g., investment). This bill would help close the gaps in the CFIUS process to account for these 21st century national security risks.

China's Rapid Military Modernization. By 2025, China will pose the greatest threat to U.S. national security of any nation, according to USMC Gen. Joe Dunford, Chairman of the Joint Chiefs of Staff. China seeks advanced U.S. technology at least in part to develop more capable military weapon systems and find vulnerabilities in our own systems. To that end, China intentionally blurs the line between its military activities and ostensibly civilian activities through its policy of "military-civilian fusion," a cornerstone of its defense reforms through which China combines its defense and civilian industrial bases for the purpose of meeting both its military and commercial demands. The military-civilian fusion policy also "appears to drive China's international acquisition of dual-use technologies and resources, and knowledge to fill domestic S&T [science and technology] gaps," according to a recent report by a private research firm. This is important context for considering China's investments in U.S. companies. The use of U.S.-derived technology to speed China's aggressive military modernization would be highly damaging to U.S. national security. China's expanding capabilities have emboldened it to take more aggressive actions in asserting its interests and territorial claims, such as accelerating construction at expanded outposts in the South China Sea and more aggressive posturing towards Taiwan.

Rationale for reform: Gaps in existing CFIUS process. The current CFIUS process is not adequately protecting against this threat vector from potential adversaries. There are clear gaps in the CFIUS process, which China is exploiting. CFIUS was not designed to stop investment-driven technology transfers, and many such transactions are occurring today, carefully designed to sidestep CFIUS' limited jurisdiction.

U.S. national security establishment backs CFIUS reform.

- Attorney General Jeff Sessions: CFIUS "is not able to be effective enough. Your legislation [FIRRMA] is first-rate. We think it has great potential to push back against the abuses and dangers we face."
- Secretary Mattis: CFIUS is outdated and "needs to be up updated to deal with today's situation."
- DNI Coats: We should do "a significant review of the current CFIUS situation to bring it up to speed."
- Admiral Rogers (NSA Director; Commander of U.S. Cyber Command): We need to reassess the CFIUS process and "make sure it's optimized for the world of today and tomorrow."

Highlights of FIRRMA. The reforms in the bill are laser-focused on national security concerns and represent a measured approach to the problem. The bill recognizes the need to preserve as much certainty and predictability for investors as possible. Specifically, the bill would:

- Expand CFIUS jurisdiction to include certain joint ventures, minority position investments, and real estate transactions near military bases (or other sensitive national security facilities).
- Update CFIUS' definition of "critical technologies" to include emerging technologies that could be essential for maintaining the U.S. technological advantage over countries that pose threats.
- Authorize CFIUS to exempt certain transactions for investors from countries that meet certain criteria.
- Create "light filings" for certain transactions; add new national security factors for CFIUS to consider.

What this bill does not do. It does not:

- Impose a ban on (or automatically block) Chinese investment transactions;
- Require CFIUS to consider investment reciprocity or economic security impacts in its analysis.
- Cover all joint ventures with Chinese entities; make any changes to CFIUS' membership.
- Require any list of countries of special concern (or any other type of country).
- Require any list of technologies or duplicate functions performed by the export control system.
- Designate specific technologies that are to be safeguarded.

Rationale for key reforms in FIRRMA

Relevant FIRRMA text – Sec. 3(a)(5)(B):

(iii) Any other investment (other than passive investment) by a foreign person in any United States critical technology company or United States critical infrastructure company, subject to regulations prescribed under subparagraph (C). . . .

(v) The contribution (other than through an ordinary customer relationship) by a United States critical technology company of both intellectual property and associated support to a foreign person through any type of arrangement, such as a joint venture, subject to regulations prescribed under subparagraph (C).

Rationale for FIRRMA's expansion of CFIUS authority to cover "contributions" (JVs, etc.) and non-controlling (i.e., non-passive) investments: FIRRMA aims to capture transactions that have, in effect, the same national security consequences as an acquisition of the U.S. company or a piece of it. Foreign investors should not be able to circumvent CFIUS and get via the "back door" something they cannot get through the "front door." The intent is not to have CFIUS take over functions that are already adequately performed by the export control system. Instead, FIRRMA is aimed primarily at transactions that go much further and allow a foreign investor to acquire an industrial/technological capability that is embodied in a U.S. business.

China's policy of aggressive "military-civil fusion" (MCF) exacerbates the risk of diversion of U.S. dual-use technologies. In order to help modernize its military, China purposely blurs the lines between military and ostensibly civilian activities, combining its defense and civilian industrial bases for the purpose of supporting both its military and commercial demands. This is important context for considering China's investments in U.S. companies, because China's military suppliers and their activities are woven right into China's commercial environment. The result of China's MCF is that the diversion of exports will be increasingly more difficult to track effectively, which greatly increases the national security risks. In essence, U.S. technology and know-how transferred to "private" Chinese companies are likely to contribute directly and materially to China's military modernization.

China has identified gaps in our relevant safeguards (CFIUS, export controls) and is exploiting them. Neither the current CFIUS process nor the export control system have proven able to address the range of national security risks inherent in Chinese investment in the U.S. CFIUS was never designed to stop investment-driven transfers of technology and related know-how, but many such transactions are occurring today, having been carefully designed to circumvent CFIUS' limited jurisdiction. Some minimal overlap between CFIUS and the export control system is necessary to close these gaps and protect national security, and CFIUS and export controls are designed to be complementary, not mutually exclusive.

The export control system would remain the first line of defense in addressing national security risks posed by certain non-controlling investments and arrangements such as joint ventures (JVs), but it also has inherent limitations. Multilateral export controls have proven ineffective thus far for many emerging technologies, because they require the U.S. to wait for international policy consensus on difficult issues. The fast pace of innovation will not wait for that, meaning that damage to U.S. national security is likely to occur in the interim. The

export control system is too bureaucratic and slow-moving to adequately address national security risks and is simply unable to keep pace with the rapid evolution of technology.

- In many cases, it fails to effectively regulate the transfer of know-how (i.e., human capital) inherent in the workforce of U.S. technology companies, especially in overseas settings.
- The risk, particularly as it relates to emerging/enabling technologies, may not yet be susceptible to categorization as required under dual-use export controls.
- Not all of the potential national security risks are related to technology transfer (e.g., supply assurance and supply chain security), and not all of the technology that may raise national security risks if conveyed with know-how is currently controlled.
- Ownership interests and JV relationships may give foreign persons placement and access that can be exploited regardless of the U.S. business's intent to comply with export control laws.
- The potential sensitivity of contributions may not come to light without CFIUS review, if a given technology is not currently controlled. In some instances, CFIUS has identified national security risks involving technologies that were not controlled for export to a given country and would not have been otherwise identified through the export control process.
- The risk may also be tied only to specific acquirers, such that a broader export control may not be warranted.
- The risk may center not on what the U.S. business intends to produce with the technology (which is typically what export controls focus on), but whether the malicious actor could use the technology for another purpose (not intended by the U.S. business).

FIRRMA includes safeguards to ensure CFIUS plays a role only when necessary. Today, where CFIUS determines that other authorities are adequate and appropriate to address the national security risks in a certain transaction, it does not take action. The same would be true with the expanded authorities that would be provided to CFIUS under FIRRMA. Not all JVs or non-controlling investments raise national security risks and, even when they do, export controls could be adjusted to address those risks in many instances. FIRRMA would expressly authorize CFIUS, through regulations, to:

- Identify the types of contributions, by technology, sector, subsector, transaction type, or other transaction characteristic, that are subject to review. This would allow CFIUS to avoid affecting transactions that do not warrant review based on potential national security risks or transactions where the risk is adequately addressed under existing authorities. This would also allow stakeholders to provide their input through the notice and comment rule-making process.
- Define circumstances in which (B)(v) contributions can be excluded because other provisions of law (including export controls) are adequate to address any national security risks.
- Identify countries to be put on a positive list, based on a variety of factors, for which transactions under (b)(ii), (iii), or (v) would be exempt from review.

Engagement with allies will be necessary to ensure some consistency in the application of any new authorities and to avoid disadvantaging U.S. companies and decreasing the strength of the U.S. innovation. Based on discussions with multiple allied governments and also news reports, several key U.S. allies are also rethinking their policies on China's acquisition of industrial capabilities that are aimed at bolstering its military capabilities. Some of them have already made adjustments without any prodding from the U.S. They are considering what other changes to make to their own safeguards and are looking to the U.S. for leadership on this. At a minimum, this list includes Japan, Australia, Canada, Germany, and the EU itself.

Foreign Investment Risk Review Modernization Act (FIRRMA)

Section-by-section summary

Sec. 1 – Short title, table of contents.

Sec. 2 – Sense of Congress.

This section would express the Sense of Congress regarding the:

- Benefits of foreign investment in the U.S. and the continuing U.S. commitment to open and fair investment policy;
- Shifting national security landscape and the need to modernize the CFIUS process;
- Critical role of CFIUS and its need for adequate resources;
- Need for more robust international outreach to allies and partners to help them establish their own processes for investment screening and to otherwise coordinate; and
- Need to collaborate with allies and partners to develop stronger multilateral export controls.

Sec. 3 – Definitions.

This section restates the entire definitions section from the current CFIUS statute, making updates to important terms and adding several new terms.

Updated terms include:

- **"Covered transaction"**:
  - The current definition only covers transactions that result in foreign "control" of the U.S. business. This definitional update broadens the purview of CFIUS by explicitly adding five new types of covered transactions:
    1) Any non-passive investment by a foreign person in any U.S. critical technology company or critical infrastructure company (subject to regulations further defining it by reference to technology, sector/subsector, transaction type, or other characteristic).
    2) The contribution by a U.S. critical technology company (other than through an ordinary customer relationship) to a foreign person of both intellectual property (IP) and associated support through a joint venture or other arrangement.
       - Subject to regulations that further define this by reference to technology, sector/subsector, transaction type, or other characteristic.
       - CFIUS would be authorized to exclude certain otherwise qualifying contributions where other U.S. Government authorities can completely address national security risks, avoiding the need to conduct wholly redundant reviews of such transactions.
    3) Any change in a foreign investor's rights regarding a U.S. business, if it could result in either foreign control of the U.S. business or in a non-passive investment (see #1).
       - This would allow CFIUS to review any circumstance where a non-controlling investment changes to a controlling investment, or where a passive investment changes to a non-passive investment. This is of particular concern where a foreign investor might design an investment to avoid CFIUS review, then later change its rights to obtain control or become non-passive.
    4) Any other transaction, transfer, agreement, or arrangement the structure of which is designed/intended to evade/circumvent CFIUS (subject to regulations).
    5) The purchase/lease by a foreign person of certain real estate located in the U.S. in close proximity to military or other USG national security facilities.
  - Exemptions for certain countries. CFIUS would be authorized to exempt certain otherwise covered transactions (#1, #2, and #5 above) if all foreign investors are from a country that meets certain criteria, such as being a U.S. treaty ally, having a mutual investment security arrangement, and having a sound CFIUS-like process of its own.

- **"Critical technologies" –** Update definition to codify essential portion of existing CFIUS regulations. Subject to new regulations, but includes technology, components, or technology items that are essential or could be essential to national security, including the following:
  - Defense articles or defense services on the United States Munitions List;
  - Certain items on the Commerce Control List;
  - Certain nuclear items, including equipment, components, technology, and facilities;
  - Certain biological and chemical agents and toxins; and
  - Other emerging technologies that could be essential for maintaining or increasing the U.S. technological advantage with respect to national security.
- **"Control" –** Update definition (subject to regulations) to codify essential portion of existing CFIUS regulations: the power to determine, direct, or decide important matters affecting an entity.

New terms include:

- **"Passive investment"**: an investment (subject to regulations):
  - that does not afford the foreign investor:
    1) Access to any nonpublic technical information, or any nontechnical information that is not available to all investors;
    2) Membership or observer rights on the board of directors; or
    3) Any involvement, other than through voting of shares, in substantive decisionmaking; and
  - Under which the foreign investor and the U.S. business do not have a parallel strategic partnership or other material financial relationship. Rationale: certain strategic partnerships, when coupled with non-controlling investment stakes, can result in avenues of significant influence, despite the lack of formal rights associated with the investment stake itself.
- **"Nonpublic technical information"**: subject to regulations, but includes information without which critical technologies cannot be designed, developed, tested, produced, or manufactured; and in a quantity sufficient to permit the design, development, testing, production, or manufacturing of such technologies.
- **"U.S. critical technology company"**: a U.S. business that produces, trades in, designs, tests, manufactures, services or develops critical technologies (subject to regulations).
- **"U.S. critical infrastructure company"**: a U.S. business that is, owns, operates, or primarily provides services to, an entity or entities that operate within a critical infrastructure sector or subsector (subject to regulations).
- **"Country of special concern"**: a country that poses a significant threat to U.S. national security interests (clarifies that no list of such countries is required).
- **"Malicious cyber-enabled activities"**: acts primarily accomplished through or facilitated by computers or other electronic devices that are reasonably likely to result in, or materially contribute to, a significant threat to U.S. national security; and that have the purpose or effect of:
  - Significantly compromising the provision of services in a critical infrastructure sector;
  - Harming, or otherwise significantly compromising the provision of services by, a computer or network in a critical infrastructure sector;
  - Causing a significant disruption to the availability of a computer or network; or
  - Causing a significant misappropriation of funds or economic resources, trade secrets, personally identifiable information, or financial information.
- **"Critical materials"**: physical materials essential to national security (subject to regulations).
- **"U.S. business"**: a person engaged in interstate commerce in the U.S.
- **"Investment"**: the acquisition of equity interest, including contingent equity interest (subject to regulations).
- **"Access"**: the ability to and opportunity to obtain information (subject to regulations).

Sec. 4 – Inclusion of partnership and side agreements in notice.
This section would require that any written notice (i.e., filing) include copies of all related partnership agreements, integration agreements, or other side agreements relating to the transaction, including any related to IP transfer.

Sec. 5 – Declarations relating to certain covered transactions.
This section would create the concept of declarations, "light" filings that could be voluntarily filed in lieu of notices for any covered transactions, would be limited to five pages in length, and would not automatically trigger a CFIUS review (unlike notices). It would require that declarations be filed 45 days prior to completion of the transaction.

Mandatory filings. This section would also mandate the filing of declarations for:

1) Certain investments by state-owned enterprises. These are transactions involving the acquisition of a voting interest of 25% or more by a foreign investor in which a foreign govt. owns a voting interest of 25% or more.
2) Other covered transactions, at the discretion of CFIUS. CFIUS would be authorized to mandate by regulation the filing of declarations for certain types of transactions, based on factors such as:
    - The technology, industry, sector, or subsector in which the U.S. business trades;
    - The difficulty of remedying the harm to national security that may result from completion of the transaction; and
    - The difficulty of obtaining information on the type of transaction through other means.

With transactions for which declarations would be mandatory, this section would:

- Allow the parties to file a regular notice instead (90 days prior to completion of the transaction); and
- Authorize CFIUS to impose penalties for noncompliance.

Upon receiving a declaration, CFIUS would have to "endeavor" to take one of three actions within 30 days:

- Request the filing of a regular notice;
- Inform the parties that, if they seek clearance of the transaction, they may file a regular notice;
- Initiate a unilateral review of the transaction; or
- Clear the transaction (and notify the parties in writing).

Sec. 6 – Stipulations regarding transactions.
This section would authorize the parties to stipulate (in either a notice or a declaration) that a transaction is a covered transaction and, if so, that it is also a foreign government-controlled transaction. In so doing, it would simplify these two steps of the review process in certain transactions by eliminating the need for this analysis, which can be time-consuming.

Sec. 7 – Authority for unilateral initiation of reviews.
This section would confirm the circumstances under which CFIUS may unilaterally initiate a review, as well as how a transaction attains "safe harbor" status. In addition, it would lower the standard for when reviews of past cleared transactions may be unilaterally initiated by eliminating the current CFIUS statute's intent requirement (regarding material breaches of conditions and mitigation agreements).

Sec. 8 – Timing for reviews and investigations.
This section would give CFIUS extra time to review each transaction by extending the overall review period from 30 days to 45 days, reducing the need for foreign investors to have to withdraw and refile CFIUS notices one or more times in transactions that necessitate a more thorough review. It would authorize CFIUS to extend any investigation for one 30-day period in extraordinary circumstances (to be defined by CFIUS in regulations), at the request of the head of a lead agency. This section would also require CFIUS to notify the parties in the event of any such extension. Lastly, in the event of a "government shutdown, it would suspend all time limitations for reviews and investigations.

Sec. 9 – Monitoring of non-notified and non-declared transactions.
This section would require CFIUS to establish a mechanism to identify any covered transactions for which a notice or declaration has not been filed and on which information is reasonably available.

Sec. 10 – Submission of certifications to Congress.
The current CFIUS statute requires CFIUS to submit a certification to Congress upon completion of a review or investigation of a transaction. This section would enhance congressional oversight of the CFIUS process by requiring CFIUS to submit its certifications to both the SSCI and HPSCI (as oversight committees for the U.S. Intelligence Community). It would also provide CFIUS with more flexibility regarding the required signatures on these certifications, easing the current restriction on delegation below the Deputy Secretary level. This section would authorize the chairperson to determine the appropriate level of official to whom the signature requirement may be delegated, and it would allow the delegation to vary based on any appropriate factor relating to a transaction. However, the requirement could not be delegated below the level of Deputy Assistant Secretary (or equivalent). For any transaction that is assessed by the Director of National Intelligence (DNI) as more likely than not to pose a threat to U.S. national security, the requirement could not be delegated below the level of Assistant Secretary (or equivalent). Lastly, this section would authorize CFIUS to "batch" the certifications and send them to Congress on a monthly basis, instead of transmitting them individually.

Sec. 11 – Analysis by Director of National Intelligence.
This section would require the DNI, for each National Security Threat Assessment (NSTA), to:

- Identify any recognized intelligence collection gaps relevant to the NSTA;
- Update the NSTA for any past cleared transaction involving a mitigation agreement, upon request by a lead agency; and
- Submit the NSTA to the SSCI and HPSCI after conclusion of action by CFIUS.

It would authorize the DNI to provide CFIUS, in lieu of full-blown NSTAs, with "Basic Threat Information" (BTI) on any certain transactions, such as those:

- For which the DNI has completed a NSTA involving each foreign investor during the previous 12 months;
- Involving the purchase/lease by a foreign person of U.S. real estate in close proximity to military or other USG national security facilities; and
- Meeting other criteria agreed upon by CFIUS and the DNI.

This section would also require CFIUS to ensure that its processes preserve the independence and objectivity of the DNI in conducting NSTAs and BTIs. Lastly, it would authorize the DNI, for any transaction, to provide CFIUS with a separate assessment of any operational impact of the transaction on the Intelligence Community and a description of any actions being taken to mitigate it.

Sec. 12 – Information sharing.
This section, in conjunction with Sec. 2, would enhance collaboration and coordination with U.S. allies/partners by clarifying that the existing rules on confidentiality do not prohibit the disclosure of:

- Information to any domestic or foreign governmental entity, if necessary for national security (and pursuant to appropriate confidentiality and classification arrangements); or
- Information that the parties have consented to be disclosed to third parties.

Sec. 13 – Action by the President.
This section slightly expands the authority of the President to take action against a transaction to protect national security, giving him/her an additional option (in addition to "suspend or prohibit"). The President would be authorized to "take any additional action" that is appropriate to address national security risks that were identified during the CFIUS review or investigation, thus limiting the possibility of the subsequent evasion of a Presidential suspension or prohibition order. This section also does some statutory housekeeping, confirming that the President's authority includes requiring divestment, when necessary to protect national security. Lastly, for transactions that CFIUS refers to the President for action prior to the

completion of an investigation (see Sec. 18), this section makes a conforming change to the timeline for the President to announce that decision.

Sec. 14 – Judicial review procedures.

The CFIUS statute exempts from judicial review certain actions of the President, including suspension/prohibition of transactions and the making of related findings. This section would extend that exemption to any designee of the President. Additionally, it would create a similar, but more limited, exemption for actions of CFIUS itself, including determinations, recommendations to the President, and various actions related to mitigation agreements or conditions, while also providing a clear process for appeal of CFIUS actions. To resolve uncertainty following the U.S. Court of Appeals for the D.C. Circuit's decision in *Ralls Corp. v. CFIUS*, 758 F.3d 296 (D.C. Cir. 2014), this section would provide that:

- Any party to the transaction may file a petition (within 60 days of the President's/CFIUS' decision), alleging that the action is a violation of a constitutional right, power, privilege, or immunity;
- A party may only file a petition if it previously filed a notice/declaration with CFIUS (or CFIUS determines one was not required), and CFIUS has completed all action;
- The D.C. Circuit has exclusive jurisdiction over any appeal (subject to review by the Supreme Court), and a determination by the court is the exclusive judicial remedy; and
- The court must decide all relevant questions bases solely on an administrative record submitted by the U.S. Govt.

Sec. 15 – Factors to be considered in taking action.

The CFIUS statute lays out 10 specific factors that CFIUS may consider when analyzing a transaction's national security implications. This section would update four of those factors and add nine new ones, providing for consideration of:

- Whether the transaction is likely to have the effect of creating new U.S. cybersecurity vulnerabilities in the U.S. or exacerbating existing ones (new factor);
- The extent to which the transaction is likely to expose personally identifiable information, genetic information, or other sensitive data of U.S. citizens to access by a foreign government/person that may exploit it in a manner that threatens national security (new factor);
- The degree to which the transaction is likely to increase the cost to the U.S. Government of acquiring or maintaining the equipment and systems that are necessary for defense, intelligence, or other national security functions (new factor);
- Whether the transaction involves a country of special concern that has a demonstrated or declared strategic goal of acquiring a type of critical technology that a U.S. business that is a party to the transaction possesses;
- Whether the transaction is likely to reduce the U.S. technological and industrial advantage, relative to any country of special concern (added to existing factor #5);
- Whether the transaction is likely to contribute to the loss of or other adverse effects on technologies that provide the U.S. a strategic national security advantage (added to existing factor #7);
- Whether the transaction is likely to result in increased reliance by the U.S. on foreign suppliers to meet national defense requirements (added to existing factor #1);
- The potential national security-related effects of the cumulative market share of any one type of infrastructure, energy asset, critical material, or critical technology by foreign persons (new factor);
- The potential national security-related effects on transportation assets, as defined in Presidential Policy Directive 21 (added to existing factor #6);
- Whether the foreign investors have a history of complying with U.S. laws/regulations, including those relating to exports, the protection of IP, and immigration, as well as adhering to contracts/agreements with U.S. Govt. entities (new factor);
- Whether the transaction is likely to result in a foreign government gaining a significant new capability to engage in malicious cyber-enabled activities against the U.S., including those designed to affect the outcome of any federal elections (new factor);

- Whether the transaction is likely to facilitate criminal or fraudulent activity affecting U.S. national security; and
- Whether the transaction is likely to expose any information regarding sensitive national security matters or sensitive procedures/operations of a federal law enforcement agency (with national security responsibilities) to an unauthorized foreign entity (new factor).

Sec. 16 – Actions by the Committee to address national security risks.

Suspension or referral of transactions. This section would grant CFIUS the authority to suspend, during a review or investigation, any transaction that may pose a risk to U.S. national security. It would also confirm CFIUS' authority to complete action on a transaction at any point during a review or investigation and refer the transaction to the President for further action against it.

Abandonment of transactions. It would give CFIUS new authority to use mitigation agreements and conditions in situations where the parties have chosen to abandon a transaction, authorizing CFIUS to negotiate, enter into or impose, and enforce any agreement or condition for the purpose of carrying out that abandonment and mitigating any U.S. national security risks that arise. This expressly confirms CFIUS' authority to accept a voluntary abandonment (including through divestment) of a transaction that it has determined poses national security concerns, without needing a public Presidential finding and order.

Interim risk in completed transactions. This section would confirm that CFIUS has the authority to use interim mitigation agreements and conditions regarding completed transactions (that have not yet undergone CFIUS review), authorizing CFIUS to negotiate, enter into or impose, and enforce any agreement or condition until CFIUS has completed action on the transaction or the President has taken action on it, for the purpose of mitigating any interim U.S. national security risks.

Standards for mitigation agreements. It would prohibit CFIUS from entering into any mitigation agreement or imposing any condition regarding a transaction unless CFIUS determines that the agreement/condition resolves any national security concerns posed by the transaction, considering whether it is reasonably calculated to be effective, allows for compliance in an appropriately verifiable way, and enables effective compliance monitoring and enforcement.

Risk-based analysis. This section also requires that a "risk-based analysis" (RBA) of a transaction and its effects on national security be conducted prior to CFIUS referring the transaction to the President for action or suspending the transaction (currently, RBAs are only required before CFIUS pursues a condition or a mitigation agreement). It further requires that the RBA include an assessment of:

- The national security threat posed by the transaction, taking into account the DNI's NSTA;
- Any related national security vulnerabilities; and
- The transaction's potential national security consequences.

It also requires that the RBA include an identification of any national security factors in subsection (f) of the statute (see Sec. 15) that are substantially implicated by the transaction. If any CFIUS member agency concludes that a transaction poses an unresolved national security concern, this section requires that agency to recommend an action and propose the requisite RBA. In the event that CFIUS fails to reach a consensus on a recommendation, it requires the CFIUS member agencies who support an alternative recommendation to produce a written justification for that recommendation and, if needed, an RBA to support it. In so doing, this section provides a clear mechanism through which CFIUS can resolve internal differences over how to handle contentious transactions.

Compliance plans. This section would also require CFIUS to formulate, adhere to, and keep updated a plan for monitoring compliance of cleared transactions involving a mitigation agreement or condition, including:

- Which dept./agency will have primary responsibility for monitoring compliance;
- How compliance will be monitored;
- How frequently compliance reviews will be conducted;

- Whether an independent entity will be utilized to conduct compliance reviews; and
- What action will be taken if the parties fail to cooperate regarding compliance monitoring.

This section also requires CFIUS, if it contracts with an independent entity from outside the U.S. Govt. to conduct compliance monitoring, to take action to prevent a conflict of interest from arising on the part of that independent entity. It would also repeal the current statutory requirement that CFIUS, in developing methods to ensure compliance of mitigation agreements, avoid placing unnecessary burdens on the parties. This section also includes a provision to confirm that U.S. district courts have jurisdiction over actions to enforce and enjoin violations of mitigation agreements, as is already the case with mitigation orders.

Noncompliance. In addition, this section would provide CFIUS with additional tools to use in the event of the parties' noncompliance with mitigation agreements or conditions:

- Negotiating a plan of action for remediating the noncompliance, with failure to abide by the plan serving as a basis for CFIUS to find a material breach;
- Requiring that the parties submit for CFIUS review any new covered transactions for 5 years; and
- Seek injunctive relief.

Sec. 17 – Modification of annual report.

This section would increase transparency by requiring several new elements in each CFIUS annual report:

- A description of the outcomes of any reviews/investigations that year, including whether a mitigation agreement was entered into or condition imposed and whether the President took any action; and
- Statistics on compliance reviews conducted, highlighting any remediation or enforcement actions taken by the Committee.

This section would prohibit the inclusion of any trade secrets or business confidential information in the public version of the annual report. It would also require sharing of the report and its classified annex with eight additional congressional committees that have major equities in the CFIUS process: the SSCI and HPSCI, the SASC and HASC, the Senate Judiciary Committee and House Judiciary Committee, and the Senate HSGAC and House HSC.

In addition, this section would establish a new Intelligence Community (IC) interagency working group on foreign investment risk, led by the DNI, and task it with preparing a biennial report, to be submitted along with the classified annex to the annual CFIUS report in even-numbered years only. The IC report would include identification, analysis, and explanation of:

- Any current or projected major national security threats regarding foreign investment;
- Any strategies used by countries of special concern to utilize foreign investment to target the acquisition of critical technologies, critical materials, or critical infrastructure; and
- Any economic espionage efforts directed at the U.S. by a foreign country, particularly a country of special concern.

Sec. 18 – Certification of notices and information.

Under paragraph (n) of the statute, each notice (and any follow-up information) submitted to CFIUS has to be accompanied by a written statement from the parties, certifying that the notice or information is accurate, complete, and compliant with the rules. This section would prohibit CFIUS from completing a review of any transaction for which such a certification is not submitted, includes false or misleading information, or omits material information. It would also authorize CFIUS, on that basis, to recommend to the President that the transaction be blocked or unwound. Lastly, this section requires CFIUS to prescribe regulations providing for the application of 18 USC 1001, which criminalizes the act of making false statements.

Sec. 19 – Funding.

This section establishes the "CFIUS Fund" and authorizes appropriations ("such sums as may be necessary to perform the functions" of CFIUS). It also authorizes CFIUS to assess and collect filing fees for any

covered transactions for which a notice is filed (but not for declarations). The exact amount would be set by CFIUS in regulations, but it would be capped at 1% of the value of the transaction or $300,000 (indexed for inflation), whichever is lesser. Amounts collected would be deposited into the CFIUS Fund to cover work on reviews, investigations, and other CFIUS activities. They would remain available until expended, and they would be in addition to any appropriations from Congress. Lastly, the chairperson would be authorized to transfer funding from the CFIUS Fund to any member agencies to address emerging needs in executing the requirements of this bill.

Sec. 20 – Centralization of certain Committee functions.
This section would authorize the Secretary of the Treasury (as CFIUS chairperson) to centralize certain CFIUS functions, including monitoring non-notified and non-declared transactions, within the Treasury Dept. to enhance CFIUS interagency coordination and collaboration.

Sec. 21 – Unified budget request.
This section would authorize the President to submit a unified budget request for CFIUS (as a component of his annual budget request for the Dept. of the Treasury), covering any or all CFIUS operations of the CFIUS member agencies and including details and amounts for each dept./agency.

Sec. 22 – Special hiring authority.
This section would authorize CFIUS member agencies to direct-hire candidates for CFIUS jobs, allowing it to bypass certain parts of the traditional hiring process that have made it difficult to identify and hire qualified people in a timely manner. CFIUS work requires individuals who have a specialized skill set, and this change would give CFIUS member agencies the ability to better recruit and hire these individuals in a timely manner, addressing a significant challenge that CFIUS agencies currently face.

Sec. 23 – Conforming amendments.
This section would make six conforming changes to the statute.

Sec. 24 – Assessment of need for additional resources for Committee.
This section would help ensure that CFIUS is fully resourced to carry out its updated statutory mandate, by requiring the President to:

- Determine whether and to what extent the expansion of CFIUS' responsibilities per this legislation necessitates additional resources for CFIUS and its members to perform their functions, and
- Include a request for any such additional resources in his/her annual budget request to Congress.

Sec. 25 – Authorization for DARPA to limit foreign access to technology through contracts and grant agreements.
This section would authorize the DARPA Director, through provisions in contracts or grant agreements, to:

- limit foreign access to technology that is the subject of the contract or grant agreement; and
- if the provision is violated, require the party to return all amounts received from DARPA.

Sec. 26 – Effective date.
This section delays the applicability of some of the bill's most significant provisions until 30 days after the CFIUS chairperson publishes in the Federal Register a determination that the necessary regulations, organizational structure, personnel, and other resources are in place to administer those provisions. However, it makes certain components of the bill effective immediately upon enactment, including certain definitions, requirements, authorities, and reporting requirements. This section also authorizes CFIUS, upon enactment and at its discretion, to conduct pilot programs to implement any authority provided under this bill.

Sec. 27 – Severability.
This section would provide that, if any provision of the bill (or application of the provision) is held to be invalid, the remaining provisions and the application of that provision to other persons shall not be affected.

GROWING SUPPORT FOR FIRRMA

Current U.S. national security leaders back FIRRMA

Secretary of Defense James Mattis (12/15/17 letter):

- "I strongly support the Foreign Investment Risk Review Modernization Act of 2017 (FIRRMA)."
- "DoD depends on critical, foundational, and emerging technologies to maintain military readiness and preserve our technological advantage over potential adversaries. FIRRMA would help close related gaps that exist in both the Committee on Foreign Investment in the United States (CFIUS) and export control processes, which are not presently keeping pace with today's rapid technological changes."
- "CFIUS plays a critical role in protecting the national security of the United States. FIRRMA greatly strengthens that protection and provides much needed CFIUS modernization."

Secretary of the Treasury Steven Mnuchin (quote provided on 12/14/17): "I support the goals of FIRRMA, which will help to ensure that CFIUS has the tools necessary to protect the national security of the United States, while simultaneously maintaining our open investment environment. I stand ready to work with Senators Cornyn, Feinstein, and Burr, the committees of jurisdiction, and other Members of Congress as this important legislation advances."

Attorney General Jeff Sessions (12/13/17 letter): "I am particularly supportive of the goals of several aspects of your proposed legislation, including but not limited to (1) the expansion of CFIUS's authority to review certain transactions that may pose national security concerns; (2) an expanded list of national security factors that CFIUS should consider; and (3) mandatory disclosures of certain investments by state-owned enterprises. . . . I know the Administration stands ready to work with you to enhance our national security."

In addition, on October 18, 2017, at a Senate Judiciary Committee hearing, Attorney General Sessions was asked by Sen. Cornyn whether he supports the effort to modernize and reform the CFIUS process. "I absolutely do. We have looked at that hard in the Department of Justice. I have talked with attorneys and agents who have investigated these cases. They are really worried about our loss of technology. We certainly need additional legislation. Just as you said, you can buy an interest in a company and gain access to the same type of technology. The CFIUS program is not able to be effective enough. Your legislation is first-rate. We think it has great potential to push back against the abuses and dangers we face. I'm excited about it, and anything I can do to say, publicly, thank you for that work and to call on Congress to move on it rapidly. You would be winning the confidence and support of people who investigate these matters every day and know what's going on. They support what you're doing, and I hope Congress can follow through."

Admiral Harry Harris, US Navy, Commander of U.S. Pacific Command (1/3/18 letter):
"Within the USPACOM area of responsibility, China represents our greatest long-term security challenge. China blurs the lines between military and civilian activity and uses its state-owned and private enterprises to exploit our open system and gain access to U.S. civil, military, and dual-use technologies. China leverages these technologies to strengthen its comprehensive national power. It is emboldened to coerce its neighbors and violate international norms and standards. This puts at risk our regional and global military advantage and influence, and ultimately our security and prosperity. Through the Department of Defense's participation in the CFIUS process, we are well aware that CFIUS is protecting America's crown jewels – our advanced technologies. I strongly support strengthening the CFIUS process via FIRRMA."

Former U.S. national security leaders back FIRRMA

Former Secretary of Defense Donald Rumsfeld (1/12/18 letter):

- "This letter is to express my support for the Foreign Investment Risk Review Modernization Act (FIRRMA). China's rise has produced a set of unprecedented, anti-free-market policies through which it is able to aggressively absorb advanced U.S. technology and know-how to fuel its continuing military modernization. In a relatively short period, China has become an industrial and technological challenge, thanks to both its illicit and licit activities, such as foreign investment and transfers of technology and know-how from U.S. companies."
- "In addition to serving twice as Secretary of Defense, I have also led corporations in the fields of pharmaceuticals and electronics, as well as served as a board member on other companies. As I understand it, FIRRMA would take a targeted and responsible approach to a set of complex issues. Under its provisions, the CFIUS process and the export control system would remain complementary. These systems need to be interoperable in order to begin to effectively address the full range of mounting national security issues regarding China's activities. FIRRMA would represent an important step towards modernizing our policies for the 21st Century. We must be clear-eyed about the implications of the transfer of industrial capabilities and we must do more than stand by and watch as China's actions challenge our national security edge."

Former Secretary of Homeland Secretary Michael Chertoff (quote provided on 12/27/17): "The bipartisan Foreign Investment Risk Review Modernization Act (FIRRMA) is a long overdue and welcome modernization of our CFIUS foreign investment review process. The Act plugs loopholes in our national security reviews, and adopts a holistic, risk-based analytic approach in evaluating foreign investments. FIRRMA recognizes the value of foreign investment in the United States, but assures that we can protect our key security technologies and interests from theft or manipulation."

Former Secretary of Defense Bill Perry (12/18/17 letter):

- "I write to express my strong support for your bipartisan legislation, the Foreign Investment Risk Review Modernization Act of 2017 (FIRRMA)."
- "China has identified gaps in the CFIUS process and export control system and is exploiting them to acquire industrial capabilities in dual-use U.S. technologies, aiding its own military modernization and weakening our U.S. defense industrial base. FIRRMA takes a measured and targeted approach to close these gaps, with reforms that are laser-focused on national security concerns."
- "In the interests of national security, I urge the enactment of this critical legislation as soon as possible."

Admiral Dennis Blair, US Navy (retired), former Director of National Intelligence and Commander of U.S. Pacific Command (quote provided on 11/21/17): "As co-chair of the Commission on the Theft of American Intellectual Property, I welcome the much-needed CFIUS reforms provided in the Foreign Investment Risk Review Modernization Act (FIRRMA), especially with regard to the inclusion of IP protection as a factor to be considered in the CFIUS review process. The IP Commission has long argued for this provision. By expanding the scope of CFIUS reviews, FIRRMA provides better tools to analyze foreign investments and thus will strengthen the protection of America intellectual property from theft by foreign actors."

General Mike Hagee, USMC (retired), former U.S. Marine Corps Commandant (12/21/17 letter):

- "China continues its aggressive campaign to use both licit and illicit means to acquire and absorb advanced U.S. technology and know-how to fuel its rapid military modernization, and we must be clear-eyed about the implications for our long-term national security."

- "CFIUS plays a critical role, as does the export control system, but neither have proven able to adequately address the range of national security risks inherent in Chinese investment in the U.S."
- "In the interests of national security, I urge the enactment of this critical legislation as soon as possible."

General Edward Rice, USAF (retired), former Vice Commander of Pacific Air Forces and Commander of U.S. Forces in Japan (12/29/17 letter):

- "I write to express my strong support for your bipartisan legislation, the Foreign Investment Risk Review Modernization Act of 2017 (FIRRMA)."
- "In this regard, the PRC [People's Republic of China] has a long history of accelerating its military development through the acquisition and integration of U.S. technology by legitimate and illegitimate means."
- "In my judgement, FIRRMA strikes the right balance between harvesting the benefits of foreign investment in the United States and safeguarding technologies that are critical to our national security interests."

General J.D. Thurman, US Army (retired), former Commander of U.S. Forces Korea and U.S. Army Forces Command (12/21/17 letter):

- "In particular, China's investment activities are contributing to a marked shift in the strategic balance between our countries and eroding the overall U.S. military advantage over potential adversaries that has underpinned our own national security and economic prosperity since the end of World War II."
- "China has identified gaps in the CFIUS process and export control system and is exploiting them to acquire industrial capabilities in dual-use U.S technologies, aiding its own military modernization and weakening our U.S. defense industrial base. FIRRMA takes a measured and targeted approach to close these gaps, with reforms that are laser-focused on national security concerns."
- "In the interests of national security, I urge the enactment of this critical legislation as soon as possible."

Private industry players back FIRRMA

Ericsson, Inc. (1/16/18 letter):

- "[W]e commend you . . . for spearheading the Foreign Investment Risk Review Modernization Act (FIRRMA). This legislation provides critical and overdue updates to the Committee of Foreign Investment in the United States (CFIUS) review process."
- "And we must ensure there are adequate safeguards in place to property vet and scrutinize the efforts by foreign entities to gain access to our markets, and our technology. In short, FIRRMA helps provide that assurance by arming CFIUS with the tools necessary to preserve our national security interests while not discouraging investment in the United States. It's an important effort in a regulatory area that requires modernization, without which will result in the potential compromise of technology developed by companies like Ericsson and in turn, our national security."

Oracle Corporation (11/8/17 letter):

- "This important legislation will modernize and update the process used by the Committee on Foreign Investment in the United States (CFIUS) to conduct reviews of transactions that could result in a foreign entity gaining access to critical technologies and related know-how, reducing the U.S. technological and military advantage over potential adversaries."

- "The current CFIUS process does not fully take into consideration evolving strategies used to bypass attempts to acquire control of American businesses in favor of alternative mechanisms to obtain access to leading edge technology via smaller investments or joint ventures. Without reform, CFIUS will fail to address the use of these techniques that circumvent an essential review process, putting at risk critical innovations that bolster and ensure our national security."

Amsted Rail Company, Inc. (1/16/18 letter): "This important legislation will modernize the ability of CFIUS to conduct reviews of transactions that could result in a foreign entity gaining access to critical technologies and our nation's critical infrastructure. . . . FIRRMA strikes a balance of protecting national security while not chilling the benefits of foreign investment in the United States. Amsted Rail agrees with the need to reform and expand the CFIUS process as set forth in FIRRMA."

The Greenbrier Companies (1/16/18 letter): "This important legislation will modernize the ability of CFIUS to conduct reviews of transactions that could result in a foreign entity gaining access to critical technologies and our nation's critical infrastructure. . . . FIRRMA strikes a balance of protecting national security while not chilling the benefits of foreign investment in the United States. Greenbrier agrees with the need to reform and expand the CFIUS process as set forth in FIRRMA."

Railway Supply Institute (11/15/17 letter):

- "This important legislation will help to modernize and update the process used by CFIUS to conduct reviews of transactions that could result in a foreign entity gaining access to critical technologies and potentially our nation's critical infrastructure."
- "RSI represents over 260 companies and acts on behalf of the largest and smallest suppliers to North American freight and passenger railroads."
- "RSI agrees with the need to reform and expand the CFIUS process as set forth in FIRRMA and we thank you for your attention to this issue and introduction of this important legislation."

China experts back FIRRMA

Dr. Larry M. Wortzel, Commissioner, U.S.-China Economic and Security Review Commission (quote provided on 10/25/17):

- "The Committee of Foreign Investment in the United States (CFIUS) was created in a time of substantially less foreign investment and to address challenges which have increased in complexity and sophistication in the last decade. Today, United States security is challenged in particular by a determined, centrally controlled effort by China to acquire the most advanced U.S. technology and to acquire large segments of our economy and industry. Senator Cornyn's Foreign Investment Risk Review Modernization Act updates the law to better protect U.S. national security assets and close loopholes in the existing statute."
- "Innovation is an important driver of U.S. economic prosperity, and U.S. laws must keep pace with a rapidly evolving tech landscape. Senator Cornyn's Foreign Investment Risk Review Modernization Act helps prepare the United States to meet these new challenges and mitigate risks posed by current and emerging security threats."

Other support from current U.S. national security leaders for CFIUS modernization

The Trump Administration's National Security Strategy (December 2017): "While maintaining an investor-friendly climate, this Administration will work with the Congress to strengthen the Committee

on Foreign Investment in the United States (CFIUS) to ensure it addresses current and future national security risks."

Secretary of Defense Jim Mattis, at a Senate Armed Services Committee (SASC) hearing on June 13, 2017, also testified that "rapid technological change" is one of several concurrent forces acting on the Defense Department, and it includes "developments in advanced computing, big data analytics, artificial intelligence, autonomy, robotics, miniaturization, additive manufacturing, meta-materials, directed energy, and hypersonics – the very technologies that ensure we will be able to fight and win the wars of the future." He recognized that many of these advances are driven by the commercial sector, and that "new commercial technologies will change society, and ultimately, they will change the character of war." When asked by Sen. Gary Peters (D-MI) whether there is "a national security benefit to taking a tougher line against certain types of investment from nations that pose a clear threat to our national security, like China," Sec. Mattis replied, "Absolutely there is. I completely agree with your view that CFIUS is outdated, sir, and needs to be updated to deal with today's situation." **USMC Gen. Joe Dunford, Chairman of the Joint Chiefs of Staff**, voiced strong agreement.

At a Senate Select Committee on Intelligence open hearing on May 12, 2017, several senior Intelligence Community officials, when asked by Sen. Cornyn whether the current CFIUS process is adequate, expressed support for the idea of CFIUS reform.

- **Dan Coats, Director of National Intelligence**, said "I certainly think that, given China's aggressive approach relative to information gathering and all the things that you mentioned merits a review of CFIUS in terms of whether or not it is -- needs to have some changes or innovations to address the aggressive Chinese actions not just against our companies, but across the world."
- **Mike Pompeo, Director of the CIA**, said that CFIUS "mostly deals with changing control transactions, purchases. There are many other ways one could invest in an entity here in the United States and exert significant control over that entity, I think that ought to be looked at."

DNI Coats, at a SASC hearing on May 23, 2017, said "we ought to do a significant review of the current CFIUS situation to bring it up to speed . . . ."

Admiral Michael Rogers, Director of the NSA (and Commander of U.S. Cyber Command), said at a SASC hearing on May 9, 2017: "I think we need to step back and reassess the CFIUS process and make sure it's optimized for the world of today and tomorrow, because I'm watching nation-states generate insight and knowledge about our processes. They understand our CFIUS structure. They understand the criteria, broadly, that we use to make broader policy decisions about, is an investment acceptable from a national security perspective. And my concern is -- you're watching some nation-states change their methodology to -- to try to get around this process."

Steven Mnuchin, Secretary of the Treasury, at a House Financial Services Committee hearing on July 27, 2017, also said this about CFIUS reform: "There are some obvious changes we need to make to CFIUS – one of which is CFIUS doesn't cover joint ventures. But as we've had the opportunity to talk about, and we look forward to working with you and others, there's a laundry list of changes that we look forward to making with you." When asked whether he agreed that this issue is pressing, he agreed that it is.

Wilbur Ross, Secretary of Commerce, at a public forum on June 12, 2017, said: "Where I think CFIUS is weak – and there's a lot of talk within the administration about trying to build it up – it doesn't deal with joint ventures and it really tends to focus more on big companies. But to me one of the real dangers is not the giant companies, but two young kids in a garage somewhere that are onto some new technology, and [CFIUS] isn't very well set up to deal with that."

Rationale for key reforms in FIRRMA

Relevant FIRRMA text – Sec. 3(a)(5)(B):

(iii) Any other investment (other than passive investment) by a foreign person in any United States critical technology company or United States critical infrastructure company, subject to regulations prescribed under subparagraph (C). . . .

(v) The contribution (other than through an ordinary customer relationship) by a United States critical technology company of both intellectual property and associated support to a foreign person through any type of arrangement, such as a joint venture, subject to regulations prescribed under subparagraph (C).

Rationale for FIRRMA's expansion of CFIUS authority to cover "contributions" (JVs, etc.) and non-controlling (i.e., non-passive) investments: FIRRMA aims to capture transactions that have, in effect, the same national security consequences as an acquisition of the U.S. company or a piece of it. Foreign investors should not be able to circumvent CFIUS and get via the "back door" something they cannot get through the "front door." The intent is not to have CFIUS take over functions that are already adequately performed by the export control system. Instead, FIRRMA is aimed primarily at transactions that go much further and allow a foreign investor to acquire an industrial/technological capability that is embodied in a U.S. business.

China's policy of aggressive "military-civil fusion" (MCF) exacerbates the risk of diversion of U.S. dual-use technologies. In order to help modernize its military, China purposely blurs the lines between military and ostensibly civilian activities, combining its defense and civilian industrial bases for the purpose of supporting both its military and commercial demands. This is important context for considering China's investments in U.S. companies, because China's military suppliers and their activities are woven right into China's commercial environment. The result of China's MCF is that the diversion of exports will be increasingly more difficult to track effectively, which greatly increases the national security risks. In essence, U.S. technology and know-how transferred to "private" Chinese companies are likely to contribute directly and materially to China's military modernization.

China has identified gaps in our relevant safeguards (CFIUS, export controls) and is exploiting them. Neither the current CFIUS process nor the export control system have proven able to address the range of national security risks inherent in Chinese investment in the U.S. CFIUS was never designed to stop investment-driven transfers of technology and related know-how, but many such transactions are occurring today, having been carefully designed to circumvent CFIUS' limited jurisdiction. Some minimal overlap between CFIUS and the export control system is necessary to close these gaps and protect national security, and CFIUS and export controls are designed to be complementary, not mutually exclusive.

The export control system would remain the first line of defense in addressing national security risks posed by certain non-controlling investments and arrangements such as joint ventures (JVs), but it also has inherent limitations. Multilateral export controls have proven ineffective thus far for many emerging technologies, because they require the U.S. to wait for international policy consensus on difficult issues. The fast pace of innovation will not wait for that, meaning that damage to U.S. national security is likely to occur in the interim. The

export control system is too bureaucratic and slow-moving to adequately address national security risks and is simply unable to keep pace with the rapid evolution of technology.

- In many cases, it fails to effectively regulate the transfer of know-how (i.e., human capital) inherent in the workforce of U.S. technology companies, especially in overseas settings.
- The risk, particularly as it relates to emerging/enabling technologies, may not yet be susceptible to categorization as required under dual-use export controls.
- Not all of the potential national security risks are related to technology transfer (e.g., supply assurance and supply chain security), and not all of the technology that may raise national security risks if conveyed with know-how is currently controlled.
- Ownership interests and JV relationships may give foreign persons placement and access that can be exploited regardless of the U.S. business's intent to comply with export control laws.
- The potential sensitivity of contributions may not come to light without CFIUS review, if a given technology is not currently controlled. In some instances, CFIUS has identified national security risks involving technologies that were not controlled for export to a given country and would not have been otherwise identified through the export control process.
- The risk may also be tied only to specific acquirers, such that a broader export control may not be warranted.
- The risk may center not on what the U.S. business intends to produce with the technology (which is typically what export controls focus on), but whether the malicious actor could use the technology for another purpose (not intended by the U.S. business).

FIRRMA includes safeguards to ensure CFIUS plays a role only when necessary. Today, where CFIUS determines that other authorities are adequate and appropriate to address the national security risks in a certain transaction, it does not take action. The same would be true with the expanded authorities that would be provided to CFIUS under FIRRMA. Not all JVs or non-controlling investments raise national security risks and, even when they do, export controls could be adjusted to address those risks in many instances. FIRRMA would expressly authorize CFIUS, through regulations, to:

- Identify the types of contributions, by technology, sector, subsector, transaction type, or other transaction characteristic, that are subject to review. This would allow CFIUS to avoid affecting transactions that do not warrant review based on potential national security risks or transactions where the risk is adequately addressed under existing authorities. This would also allow stakeholders to provide their input through the notice and comment rule-making process.
- Define circumstances in which (B)(v) contributions can be excluded because other provisions of law (including export controls) are adequate to address any national security risks.
- Identify countries to be put on a positive list, based on a variety of factors, for which transactions under (b)(ii), (iii), or (v) would be exempt from review.

Engagement with allies will be necessary to ensure some consistency in the application of any new authorities and to avoid disadvantaging U.S. companies and decreasing the strength of the U.S. innovation. Based on discussions with multiple allied governments and also news reports, several key U.S. allies are also rethinking their policies on China's acquisition of industrial capabilities that are aimed at bolstering its military capabilities. Some of them have already made adjustments without any prodding from the U.S. They are considering what other changes to make to their own safeguards and are looking to the U.S. for leadership on this. At a minimum, this list includes Japan, Australia, Canada, Germany, and the EU itself.

Updated on December 14, 2017

FOREIGN INVESTMENT RISK REVIEW MODERNIZATION ACT (FIRRMA), S.2098

Bottom Line Up Front. China is weaponizing its investment in the U.S. to exploit national security vulnerabilities, including the back-door transfer of dual-use U.S technology and related know-how, aiding China's military modernization and weakening the U.S. defense industrial base. This has exposed serious gaps in the existing CFIUS process, and the real impacts to our national security may not be fully realized for years to come. These developments jeopardize the ability of the U.S. to maintain the overall military advantage over potential adversaries that has underpinned our national security and economic prosperity since at least the end of World War II.

Highlights of FIRRMA. The bill's reforms are laser-focused on national security concerns and represent a measured and targeted approach to the problem. It recognizes the need to preserve as much certainty and predictability for investors as possible, but also to distinguish between investments that are truly financially motivated (seeking appreciation in value) and investments that are strategically motivated (e.g., seeking to advance China's long-term military modernization or other strategic objectives). Specifically, the bill would:

- Expand CFIUS jurisdiction to include certain joint ventures, minority-position investments, and real estate transactions near military bases (or other sensitive national security facilities).
- Update CFIUS' definition of "critical technologies" to include emerging technologies that could be essential for maintaining the U.S. technological advantage over countries such as China, that pose threats to our national security.
- Authorize CFIUS to exempt certain transactions if all foreign investors are from a country that meets criteria, such as being a U.S. treaty ally and having a mutual investment security arrangement.
- Create "light filings" for certain types of transactions.
- Add new national security factors for CFIUS to consider in its analyses.

What this bill does not do. It does not:

- Impose a ban on Chinese investment in the U.S.
- Cover all joint ventures with Chinese entities.
- Automatically block any transactions (it only makes certain transactions subject to review).
- Require CFIUS to consider investment reciprocity or economic security impacts in its analysis.
- Require any list of countries of special concern (or any other type of country).
- Require any list of technologies or duplicate the entire export control system.
- Designate specific technologies that are to be safeguarded.
- Make any changes to CFIUS' membership.

Strategic Context. By 2025, China will pose the greatest threat to U.S. national security of any nation, according to USMC Gen. Joe Dunford, Chairman of the Joint Chiefs of Staff. Part of the problem is that, for years, China has been vacuuming up U.S. technology however it can, including by stealing it, reverse engineering it, or acquiring or otherwise investing in companies that develop it. China has found the gaps in existing U.S. mechanisms aimed at preventing dangerous technology transfers, including the Committee on Foreign Investment in the United States (CFIUS) process and the export control system, and it is now working to exploit those gaps.

We need to take a tougher line against certain investments from China, particularly in cutting-edge American companies, because their barrage of investments is aimed, at least in part, on eliminating our military edge. Left unchecked, China's aggressive investment in leading-edge American technology companies will further erode U.S. military superiority and undermine the U.S. defense industrial base. The U.S. needs a clear-eyed policy on what types of investment are acceptable from nations that pose a military threat, such as China. This bill would modernize the CFIUS process and account for these 21st century risks to national security.

China's Campaign to Harvest Advanced U.S. Technology. In recent years, China has embarked on a campaign to systematically vacuum up advanced U.S. technology using various means, including gaming

the export control system, taking advantage of universities and other research institutions, and theft through cyber and other means. According to the U.S.-China Economic and Security Review Commission, in its 2016 report: "China appears to be conducting a campaign of commercial espionage against U.S. companies involving a combination of cyber espionage and human infiltration to systematically penetrate the information systems of U.S. companies to steal their intellectual property, devalue them, and acquire them at dramatically reduced prices."

Today, China is using investment as a means to the same end – to gain access to U.S. technology that it wants. China has figured out how to exploit the open U.S. investment system in ways that could have serious long-term ramifications for our national security. The unprecedented level of Chinese foreign direct investment (FDI) in the U.S., mostly in sensitive, high-tech industries, is cause for serious concern. In 2016, Chinese entities invested a record $46 billion in the U.S. economy, triple what they invested the prior year and ten times what they invested five years ago. In fact, the Chinese government has a centralized and deliberate FDI strategy, through which it seeks to make Chinese firms globally competitive in ways that will undermine fair competition, erode U.S. commercial and military technological advantages, and increase U.S. dependence on foreign production.

Both state-owned and privately owned Chinese entities investing in the United States present significant risks to national security. The true extent of Chinese state ownership or influence is often unclear, but the Chinese government exerts influence in a variety of indirect ways, including through Chinese Communist Party representatives and legal ambiguities embedded in the underlying corporate structure of private Chinese companies and joint ventures with western firms. So-called private companies are still subject to frequent meddling by the Chinese government and are highly susceptible to being co-opted or coerced by the Chinese Communist Party. As such, private Chinese investors who are allowed to buy high-tech U.S. companies could easily be compelled to use that U.S. technology in ways that would be detrimental to U.S. national security. Under Chinese law, Chinese companies have no real ability to resist their government, if it seeks assistance or cooperation. The Chinese Communist Party is also creating new tools, such as behavior reports and "social credit" ratings, for gaining cooperation from Chinese citizens.

China's Unprecedented, State-Driven Industrial Overreach. China is currently implementing "Made in China 2025" (MIC 2025), a 10-year roadmap that aims to transform China into a leader in advanced manufacturing. According to analysis by the U.S. Chamber of Commerce, MIC 2025 targets 10 strategic sectors, including next-generation information technology, aviation, rail, and new energy vehicles; and provides preferential access to capital to Chinese companies "to promote their indigenous R&D capabilities, support their ability to acquire technology from abroad, and enhance their overall competitiveness." China targets these industries with the goal of acquiring the know-how for its own domestic companies. To skip the necessary stages of technological development, Chinese companies—with state support, guidance, and capital—are using their investments to generate large-scale technology transfer back to China of cutting-edge U.S. technologies.

The Obama Administration recognized this problem and began to lay the foundation for reform. In November 2016, then-Secretary of Commerce Penny Pritzker spoke about the importance of the U.S. semiconductor industry and publicly criticized the Chinese government for its ongoing campaign to "spend $150 billion to expand the share of Chinese-made integrated circuits in its market from 9 percent to 70 percent by 2025." She said that this "unprecedented state-driven interference would distort the market and undermine the innovation ecosystem." Rebuking China further, she said "no government should require technology transfer, joint-venture, or localization as a quid-pro-quo for market access."

In January 2017, President Obama's Council of Advisors on Science and Technology presented him with a report, entitled "Ensuring Long-Term U.S. Leadership in Semiconductors." The report found that "Chinese industrial policies in this sector, as they are unfolding in practice, pose real threats to semiconductor innovation and U.S. national security." It also made several recommendations, including that the U.S. should join "with allies to coordinate and strengthen inward investment security and export controls" and

"calibrate its application of national-security controls in response to Chinese industrial policy aimed at undermining U.S. security."

2017 DoD study: "China's Technology Transfer Strategy." In the Fall of 2016, under the leadership of then-Secretary of Defense Ashton Carter, DoD's Defense Innovation Unit Experimental (DIUx) launched a study exploring China's participation in venture capital deals involving early-stage technology companies. The study, completed in March 2017, found the following:

- Chinese participation in venture-backed U.S. startups is at a record level of 7-10% of all venture deals done and has grown quite rapidly in the past five years.
- The dual-use technologies that China is investing in – such as artificial intelligence, autonomous vehicles, augmented/virtual reality, robotics, and blockchain technology – are some of the same ones that are of interest to the Defense Department for ensuring the technological superiority of the U.S. military.
- Because the U.S. economy is open, foreign investors, including those from China, are able to invest in the newest and most relevant technologies we are developing for the future and gain experience with those technologies at the same rate the U.S. does.
- If we allow China access to these same technologies concurrently, then not only may we lose our technological superiority but we may even be facilitating China's technological superiority. Preserving our technological superiority and economic capacity requires urgent action today.
- The U.S. government lacks a holistic view of how fast this massive technology transfer to China is occurring, the level of Chinese investment in U.S. technology, or what technologies we should be protecting. It also lacks a comprehensive policy and the tools to address it.
- The U.S. government does not currently monitor or restrict venture investing and the potential transfer of early-stage technology know-how. CFIUS is only partially effective, and problematic investments occur beyond its jurisdiction.
    - Many transaction types, such as joint ventures, minority investments and purchased assets from bankruptcies, are effective for transferring technology but are outside of CFIUS' purview.
- Export controls are the other principal tool to inhibit technology transfer to undesirable countries, but they are only partially effective and were not designed to govern early-stage technologies or investment activity.
- The U.S. military has several areas of risk resulting from the scale of China's investments and its technology transfer:
    - Supply chains for military equipment/services are increasingly owned by Chinese firms;
    - China has made targeted investments to close the gap in capabilities between its military and the U.S. in key areas, such as jet engine design; and
    - Industrial espionage and cyber theft mean key defense designs are in Chinese hands.

The DIUx study recommends that the U.S. Government:

- Expand the scope of CFIUS to include any commercial activity that could result in technology transfer such as venture investing and to restrict investments and acquisitions of U.S. companies that own technologies the DOD identifies as critical to national security.
- Restrict investments by China in the critical technologies identified by DOD.

The Defense Department, through its DIUx study, clearly recognizes the risks here. China is pursuing leading-edge U.S. technologies, such as artificial intelligence, that have potential military applications. These technologies are so new that our export control system has not yet figured out how to cover them, which is part of the reason they are slipping through the gaps in the existing safeguards. If we do not adequately protect our advanced technology, the ramifications for our national security could be severe.

China's Rapid Military Modernization. There can be no doubt that China seeks advanced U.S. technology at least in part to develop and build more capable military weapon systems for itself and also to

identify vulnerabilities in our own systems. The use of U.S.-derived technology to speed China's aggressive military modernization would be highly damaging to U.S. national security. In order to help modernize its military, China is purposely blurring the distinction between its military activities and its ostensibly civilian activities through its policy of "military-civilian fusion" (MCF). In so doing, China combines its defense and civilian industrial bases for the purpose of supporting both its military and commercial demands. This is important context for considering China's acquisitions and other investments in U.S. companies.

According to a December 2016 report on MCF by China experts at Pointe Bello, a U.S. research firm:

- The MCF concept is a cornerstone of China's defense reforms. It is shaping China's economic and foreign policies and the strategies of state-owned defense industrial enterprises.
- Because MCF policies intentionally blur the lines between military and civilian entities, the motivations driving ostensibly commercial ventures and or research activities of defense industrial enterprises warrant greater scrutiny.
- MCF policies, in part, appear to drive China's international acquisition of dual-use technologies and resources, and knowledge to fill domestic defense S&T gaps. Acquiring and absorbing foreign technologies has long been a key part of China's military modernization.
- Foreign acquisitions executed by state-owned defense industrial enterprises appear consistent with Chinese industrial policies for introducing, digesting, and assimilating technologies that lead to "re-innovated" products (IDAR). China's IDAR-related policies:
    - Actively seek bilateral and multilateral technical cooperation;
    - Help Chinese firms "go global" in order to gain access to foreign R&D knowledge; and
    - Attract multinationals to establish R&D institutes and facilities in China
- AVIC, a Chinese state-owned enterprise and the sole supplier of aircraft to the Chinese military, operates in line with China's MCF strategy. It has acquired Western companies with valuable dual-use technologies, and its investments appear to target financially distressed small and medium sized companies with advanced dual-use technologies, R&D capabilities, and technical manufacturing expertise. AVIC receives financial support from the Chinese government to execute its M&A and industrial development activities.

In the field of high performance computing (HPC, i.e., "supercomputing"), China has attained near-peer status with the U.S., according to a December 2016 report by a joint NSA-DOE working group. The group also found that:

- Future U.S. leadership in HPC will be challenged by the Chinese. Loss of leadership in HPC could significantly reduce U.S. nuclear deterrence.
- National security requires the best computing available, and loss of leadership in HPC will severely compromise our national security. HPC plays a vital role in the design, development or analysis of many – perhaps almost all – modern weapon systems and national security systems: e.g., nuclear weapons, cyber, ships, aircraft, encryption, missile defense, precision strike capability, and hypersonics.
- Personal email and private information, social networks, and the emerging Internet of Things are all subject to even greater privacy risks if offshore entities have superior HPC analytics or control the data / information markets.

China's military capabilities continue to grow more rapidly than previously anticipated, steadily eroding the U.S. military's technological edge. With significantly more state resources devoted to defense, the Chinese military has evolved from an infantry-heavy, low-tech force to a high-tech, networked force with an emphasis on joint operations, naval capabilities, air power, and improvements in maintenance and logistics. Most concerning, China's expanding capabilities and narrowing of the technological gap with the U.S. have emboldened it to take more aggressive actions in asserting its interests and territorial claims in the South and East China Seas in recent years, such as accelerating construction at its expanded outposts in the South China Sea and more aggressive posturing towards Taiwan.

Foreign Encroachment on Military Installations. DoD also recognizes the related problem posed by foreign acquisition of resources or land assets in proximity to sensitive military installations and training ranges in the U.S., which remains a significant national security concern. In its 2016 Sustainable Ranges report, the DoD recognized that "Any development or investment near a critical training asset provides an opportunity for persistent visual and electronic observation of tactics, techniques, and procedures (TTP) training. Existing statutory mechanisms do not cover all categories of proposed transactions or projects with the potential to result in adverse impacts to military readiness and national security."

CFIUS is an interagency committee of the U.S. Government that vets foreign investments in the U.S. economy for national security risks. Through CFIUS, Congress has given the President the authority to block or unwind foreign investment transactions, but only when he believes that the foreign investor who would exercise control of the U.S. company might take action that threatens to impair the national security. The current statute gives CFIUS a great deal of latitude and flexibility in determining whether a transaction endangers national security and has resulted in a presumption of approval. However, it limits what types of investment transactions that CFIUS can review.

Rationale for reform: Gaps in existing CFIUS process. The current CFIUS process, last updated by Congress 10 years ago, is not adequately guarding against this threat vector from China and other potential adversaries. There are clear gaps in the process, and China is exploiting those. CFIUS was never designed to stop investment-driven technology transfers, and many such transactions are occurring today, having been carefully designed to sidestep CFIUS' limited jurisdiction.

First, the statutory definition of **"covered transaction" is too narrow and restricts CFIUS' jurisdiction to the point where problematic transactions escape review** and cannot be stopped. For example, CFIUS' main test for jurisdiction is the "control" test, i.e., whether the transaction would give the foreign investor "control" of the U.S. business. This concept is outdated and does not reflect the investment transactions that China is presently pursuing, including minority-position investments and joint ventures, both of which can afford investors access to sensitive technologies and/or trade secrets. These types of creative investment arrangements, which U.S. companies are sometimes pressured into, have become effective ways for China to both circumvent CFIUS review and gain indirect access to technology that could aid China's military modernization.

Second, the statute **fails to adequately recognize the emerging technologies and related know-how** that our nation will need to maintain future military superiority. Nations such as China that pose national security threats must not be allowed to harvest these early-stage technologies, which are pre-production, pre-commercialized, and in most cases lie beyond the reach of our export control system. The export control system is bureaucratic, slow-moving, fails to keep pace with rapidly changing technology, and also fail to effectively regulate the transfer of know-how (i.e., human capital) that is inherent in the workforce of U.S. technology companies. This is the type of technology China seeks and, unless the policy changes, unfortunately some of that technology is likely to be adapted and integrated onto China's weapon systems in the future and used against the U.S. military, should the U.S. ever have to face China in a future conflict.

Third, the statute **fails to ensure accountability for compliance on mitigation agreements**, which have been used aggressively in the past to "get to yes" and draw down the national security risk on a given transaction. These agreements are unevenly enforced, and cheating remains entirely possible.

FOREIGN INVESTMENT RISK REVIEW MODERNIZATION ACT (FIRRMA)

Bottom Line Up Front. Gaps in the CFIUS process have allowed China to weaponize investment to achieve the back-door transfer of dual-use U.S technology and related know-how, aiding China's military modernization and eventually further shrinking the U.S. defense industrial base. This jeopardizes the ability of the United States to maintain the overall military advantage over potential adversaries that has underpinned our national security and economic prosperity since at least the end of World War II. China is vacuuming up U.S. technology however it can, through both illicit and licit means (e.g., investment). This bill would help close the gaps in the CFIUS process to account for these 21st century national security risks.

China's Rapid Military Modernization. By 2025, China will pose the greatest threat to U.S. national security of any nation, according to USMC Gen. Joe Dunford, Chairman of the Joint Chiefs of Staff. China seeks advanced U.S. technology at least in part to develop more capable military weapon systems and find vulnerabilities in our own systems. To that end, China intentionally blurs the line between its military activities and ostensibly civilian activities through its policy of "military-civilian fusion," a cornerstone of its defense reforms through which China combines its defense and civilian industrial bases for the purpose of meeting both its military and commercial demands. The military-civilian fusion policy also "appears to drive China's international acquisition of dual-use technologies and resources, and knowledge to fill domestic S&T [science and technology] gaps," according to a recent report by a private research firm. This is important context for considering China's investments in U.S. companies. The use of U.S.-derived technology to speed China's aggressive military modernization would be highly damaging to U.S. national security. China's expanding capabilities have emboldened it to take more aggressive actions in asserting its interests and territorial claims, such as accelerating construction at expanded outposts in the South China Sea and more aggressive posturing towards Taiwan.

Rationale for reform: Gaps in existing CFIUS process. The current CFIUS process is not adequately protecting against this threat vector from potential adversaries. There are clear gaps in the CFIUS process, which China is exploiting. CFIUS was not designed to stop investment-driven technology transfers, and many such transactions are occurring today, carefully designed to sidestep CFIUS' limited jurisdiction.

U.S. national security establishment backs CFIUS reform.

- Attorney General Jeff Sessions: CFIUS "is not able to be effective enough. Your legislation [FIRRMA] is first-rate. We think it has great potential to push back against the abuses and dangers we face."
- Secretary Mattis: CFIUS is outdated and "needs to be up updated to deal with today's situation."
- DNI Coats: We should do "a significant review of the current CFIUS situation to bring it up to speed."
- Admiral Rogers (NSA Director; Commander of U.S. Cyber Command): We need to reassess the CFIUS process and "make sure it's optimized for the world of today and tomorrow."

Highlights of FIRRMA. The reforms in the bill are laser-focused on national security concerns and represent a measured approach to the problem. The bill recognizes the need to preserve as much certainty and predictability for investors as possible. Specifically, the bill would:

- Expand CFIUS jurisdiction to include certain joint ventures, minority position investments, and real estate transactions near military bases (or other sensitive national security facilities).
- Update CFIUS' definition of "critical technologies" to include emerging technologies that could be essential for maintaining the U.S. technological advantage over countries that pose threats.
- Authorize CFIUS to exempt certain transactions for investors from countries that meet certain criteria.
- Create "light filings" for certain transactions; add new national security factors for CFIUS to consider.

What this bill does not do. It does not:

- Impose a ban on (or automatically block) Chinese investment transactions;
- Require CFIUS to consider investment reciprocity or economic security impacts in its analysis.
- Cover all joint ventures with Chinese entities; make any changes to CFIUS' membership.
- Require any list of countries of special concern (or any other type of country).
- Require any list of technologies or duplicate functions performed by the export control system.
- Designate specific technologies that are to be safeguarded.

Rationale for key reforms in FIRRMA

Relevant FIRRMA text – Sec. 3(a)(5)(B):

(iii) Any other investment (other than passive investment) by a foreign person in any United States critical technology company or United States critical infrastructure company, subject to regulations prescribed under subparagraph (C). . . .

(v) The contribution (other than through an ordinary customer relationship) by a United States critical technology company of both intellectual property and associated support to a foreign person through any type of arrangement, such as a joint venture, subject to regulations prescribed under subparagraph (C).

Rationale for FIRRMA's expansion of CFIUS authority to cover "contributions" (JVs, etc.) and non-controlling (i.e., non-passive) investments: FIRRMA aims to capture transactions that have, in effect, the same national security consequences as an acquisition of the U.S. company or a piece of it. Foreign investors should not be able to circumvent CFIUS and get via the "back door" something they cannot get through the "front door." The intent is not to have CFIUS take over functions that are already adequately performed by the export control system. Instead, FIRRMA is aimed primarily at transactions that go much further and allow a foreign investor to acquire an industrial/technological capability that is embodied in a U.S. business.

China's policy of aggressive "military-civil fusion" (MCF) exacerbates the risk of diversion of U.S. dual-use technologies. In order to help modernize its military, China purposely blurs the lines between military and ostensibly civilian activities, combining its defense and civilian industrial bases for the purpose of supporting both its military and commercial demands. This is important context for considering China's investments in U.S. companies, because China's military suppliers and their activities are woven right into China's commercial environment. The result of China's MCF is that the diversion of exports will be increasingly more difficult to track effectively, which greatly increases the national security risks. In essence, U.S. technology and know-how transferred to "private" Chinese companies are likely to contribute directly and materially to China's military modernization.

China has identified gaps in our relevant safeguards (CFIUS, export controls) and is exploiting them. Neither the current CFIUS process nor the export control system have proven able to address the range of national security risks inherent in Chinese investment in the U.S. CFIUS was never designed to stop investment-driven transfers of technology and related know-how, but many such transactions are occurring today, having been carefully designed to circumvent CFIUS' limited jurisdiction. Some minimal overlap between CFIUS and the export control system is necessary to close these gaps and protect national security, and CFIUS and export controls are designed to be complementary, not mutually exclusive.

The export control system would remain the first line of defense in addressing national security risks posed by certain non-controlling investments and arrangements such as joint ventures (JVs), but it also has inherent limitations. Multilateral export controls have proven ineffective thus far for many emerging technologies, because they require the U.S. to wait for international policy consensus on difficult issues. The fast pace of innovation will not wait for that, meaning that damage to U.S. national security is likely to occur in the interim. The

export control system is too bureaucratic and slow-moving to adequately address national security risks and is simply unable to keep pace with the rapid evolution of technology.

- In many cases, it fails to effectively regulate the transfer of know-how (i.e., human capital) inherent in the workforce of U.S. technology companies, especially in overseas settings.
- The risk, particularly as it relates to emerging/enabling technologies, may not yet be susceptible to categorization as required under dual-use export controls.
- Not all of the potential national security risks are related to technology transfer (e.g., supply assurance and supply chain security), and not all of the technology that may raise national security risks if conveyed with know-how is currently controlled.
- Ownership interests and JV relationships may give foreign persons placement and access that can be exploited regardless of the U.S. business's intent to comply with export control laws.
- The potential sensitivity of contributions may not come to light without CFIUS review, if a given technology is not currently controlled. In some instances, CFIUS has identified national security risks involving technologies that were not controlled for export to a given country and would not have been otherwise identified through the export control process.
- The risk may also be tied only to specific acquirers, such that a broader export control may not be warranted.
- The risk may center not on what the U.S. business intends to produce with the technology (which is typically what export controls focus on), but whether the malicious actor could use the technology for another purpose (not intended by the U.S. business).

FIRRMA includes safeguards to ensure CFIUS plays a role only when necessary. Today, where CFIUS determines that other authorities are adequate and appropriate to address the national security risks in a certain transaction, it does not take action. The same would be true with the expanded authorities that would be provided to CFIUS under FIRRMA. Not all JVs or non-controlling investments raise national security risks and, even when they do, export controls could be adjusted to address those risks in many instances. FIRRMA would expressly authorize CFIUS, through regulations, to:

- Identify the types of contributions, by technology, sector, subsector, transaction type, or other transaction characteristic, that are subject to review. This would allow CFIUS to avoid affecting transactions that do not warrant review based on potential national security risks or transactions where the risk is adequately addressed under existing authorities. This would also allow stakeholders to provide their input through the notice and comment rule-making process.
- Define circumstances in which (B)(v) contributions can be excluded because other provisions of law (including export controls) are adequate to address any national security risks.
- Identify countries to be put on a positive list, based on a variety of factors, for which transactions under (b)(ii), (iii), or (v) would be exempt from review.

Engagement with allies will be necessary to ensure some consistency in the application of any new authorities and to avoid disadvantaging U.S. companies and decreasing the strength of the U.S. innovation. Based on discussions with multiple allied governments and also news reports, several key U.S. allies are also rethinking their policies on China's acquisition of industrial capabilities that are aimed at bolstering its military capabilities. Some of them have already made adjustments without any prodding from the U.S. They are considering what other changes to make to their own safeguards and are looking to the U.S. for leadership on this. At a minimum, this list includes Japan, Australia, Canada, Germany, and the EU itself.

Foreign Investment Risk Review Modernization Act (FIRRMA)

Section-by-section summary

Sec. 1 – Short title, table of contents.

Sec. 2 – Sense of Congress.

This section would express the Sense of Congress regarding the:

- Benefits of foreign investment in the U.S. and the continuing U.S. commitment to open and fair investment policy;
- Shifting national security landscape and the need to modernize the CFIUS process;
- Critical role of CFIUS and its need for adequate resources;
- Need for more robust international outreach to allies and partners to help them establish their own processes for investment screening and to otherwise coordinate; and
- Need to collaborate with allies and partners to develop stronger multilateral export controls.

Sec. 3 – Definitions.

This section restates the entire definitions section from the current CFIUS statute, making updates to important terms and adding several new terms.

Updated terms include:

- **"Covered transaction"**:
  - The current definition only covers transactions that result in foreign "control" of the U.S. business. This definitional update broadens the purview of CFIUS by explicitly adding five new types of covered transactions:
    1) Any non-passive investment by a foreign person in any U.S. critical technology company or critical infrastructure company (subject to regulations further defining it by reference to technology, sector/subsector, transaction type, or other characteristic).
    2) The contribution by a U.S. critical technology company (other than through an ordinary customer relationship) to a foreign person of both intellectual property (IP) and associated support through a joint venture or other arrangement.
       - Subject to regulations that further define this by reference to technology, sector/subsector, transaction type, or other characteristic.
       - CFIUS would be authorized to exclude certain otherwise qualifying contributions where other U.S. Government authorities can completely address national security risks, avoiding the need to conduct wholly redundant reviews of such transactions.
    3) Any change in a foreign investor's rights regarding a U.S. business, if it could result in either foreign control of the U.S. business or in a non-passive investment (see #1).
       - This would allow CFIUS to review any circumstance where a non-controlling investment changes to a controlling investment, or where a passive investment changes to a non-passive investment. This is of particular concern where a foreign investor might design an investment to avoid CFIUS review, then later change its rights to obtain control or become non-passive.
    4) Any other transaction, transfer, agreement, or arrangement the structure of which is designed/intended to evade/circumvent CFIUS (subject to regulations).
    5) The purchase/lease by a foreign person of certain real estate located in the U.S. in close proximity to military or other USG national security facilities.
  - Exemptions for certain countries. CFIUS would be authorized to exempt certain otherwise covered transactions (#1, #2, and #5 above) if all foreign investors are from a country that meets certain criteria, such as being a U.S. treaty ally, having a mutual investment security arrangement, and having a sound CFIUS-like process of its own.

- **"Critical technologies" –** Update definition to codify essential portion of existing CFIUS regulations. Subject to new regulations, but includes technology, components, or technology items that are essential or could be essential to national security, including the following:
  - Defense articles or defense services on the United States Munitions List;
  - Certain items on the Commerce Control List;
  - Certain nuclear items, including equipment, components, technology, and facilities;
  - Certain biological and chemical agents and toxins; and
  - Other emerging technologies that could be essential for maintaining or increasing the U.S. technological advantage with respect to national security.
- **"Control" –** Update definition (subject to regulations) to codify essential portion of existing CFIUS regulations: the power to determine, direct, or decide important matters affecting an entity.

New terms include:

- **"Passive investment"**: an investment (subject to regulations):
  - that does not afford the foreign investor:
    1) Access to any nonpublic technical information, or any nontechnical information that is not available to all investors;
    2) Membership or observer rights on the board of directors; or
    3) Any involvement, other than through voting of shares, in substantive decisionmaking; and
  - Under which the foreign investor and the U.S. business do not have a parallel strategic partnership or other material financial relationship. Rationale: certain strategic partnerships, when coupled with non-controlling investment stakes, can result in avenues of significant influence, despite the lack of formal rights associated with the investment stake itself.
- **"Nonpublic technical information"**: subject to regulations, but includes information without which critical technologies cannot be designed, developed, tested, produced, or manufactured; and in a quantity sufficient to permit the design, development, testing, production, or manufacturing of such technologies.
- **"U.S. critical technology company"**: a U.S. business that produces, trades in, designs, tests, manufactures, services or develops critical technologies (subject to regulations).
- **"U.S. critical infrastructure company"**: a U.S. business that is, owns, operates, or primarily provides services to, an entity or entities that operate within a critical infrastructure sector or subsector (subject to regulations).
- **"Country of special concern"**: a country that poses a significant threat to U.S. national security interests (clarifies that no list of such countries is required).
- **"Malicious cyber-enabled activities"**: acts primarily accomplished through or facilitated by computers or other electronic devices that are reasonably likely to result in, or materially contribute to, a significant threat to U.S. national security; and that have the purpose or effect of:
  - Significantly compromising the provision of services in a critical infrastructure sector;
  - Harming, or otherwise significantly compromising the provision of services by, a computer or network in a critical infrastructure sector;
  - Causing a significant disruption to the availability of a computer or network; or
  - Causing a significant misappropriation of funds or economic resources, trade secrets, personally identifiable information, or financial information.
- **"Critical materials"**: physical materials essential to national security (subject to regulations).
- **"U.S. business"**: a person engaged in interstate commerce in the U.S.
- **"Investment"**: the acquisition of equity interest, including contingent equity interest (subject to regulations).
- **"Access"**: the ability to and opportunity to obtain information (subject to regulations).

Sec. 4 – Inclusion of partnership and side agreements in notice.
This section would require that any written notice (i.e., filing) include copies of all related partnership agreements, integration agreements, or other side agreements relating to the transaction, including any related to IP transfer.

Sec. 5 – Declarations relating to certain covered transactions.
This section would create the concept of declarations, "light" filings that could be voluntarily filed in lieu of notices for any covered transactions, would be limited to five pages in length, and would not automatically trigger a CFIUS review (unlike notices). It would require that declarations be filed 45 days prior to completion of the transaction.

Mandatory filings. This section would also mandate the filing of declarations for:

1) Certain investments by state-owned enterprises. These are transactions involving the acquisition of a voting interest of 25% or more by a foreign investor in which a foreign govt. owns a voting interest of 25% or more.
2) Other covered transactions, at the discretion of CFIUS. CFIUS would be authorized to mandate by regulation the filing of declarations for certain types of transactions, based on factors such as:
    - The technology, industry, sector, or subsector in which the U.S. business trades;
    - The difficulty of remedying the harm to national security that may result from completion of the transaction; and
    - The difficulty of obtaining information on the type of transaction through other means.

With transactions for which declarations would be mandatory, this section would:

- Allow the parties to file a regular notice instead (90 days prior to completion of the transaction); and
- Authorize CFIUS to impose penalties for noncompliance.

Upon receiving a declaration, CFIUS would have to "endeavor" to take one of three actions within 30 days:

- Request the filing of a regular notice;
- Inform the parties that, if they seek clearance of the transaction, they may file a regular notice;
- Initiate a unilateral review of the transaction; or
- Clear the transaction (and notify the parties in writing).

Sec. 6 – Stipulations regarding transactions.
This section would authorize the parties to stipulate (in either a notice or a declaration) that a transaction is a covered transaction and, if so, that it is also a foreign government-controlled transaction. In so doing, it would simplify these two steps of the review process in certain transactions by eliminating the need for this analysis, which can be time-consuming.

Sec. 7 – Authority for unilateral initiation of reviews.
This section would confirm the circumstances under which CFIUS may unilaterally initiate a review, as well as how a transaction attains "safe harbor" status. In addition, it would lower the standard for when reviews of past cleared transactions may be unilaterally initiated by eliminating the current CFIUS statute's intent requirement (regarding material breaches of conditions and mitigation agreements).

Sec. 8 – Timing for reviews and investigations.
This section would give CFIUS extra time to review each transaction by extending the overall review period from 30 days to 45 days, reducing the need for foreign investors to have to withdraw and refile CFIUS notices one or more times in transactions that necessitate a more thorough review. It would authorize CFIUS to extend any investigation for one 30-day period in extraordinary circumstances (to be defined by CFIUS in regulations), at the request of the head of a lead agency. This section would also require CFIUS to notify the parties in the event of any such extension. Lastly, in the event of a "government shutdown, it would suspend all time limitations for reviews and investigations.

Sec. 9 – Monitoring of non-notified and non-declared transactions.
This section would require CFIUS to establish a mechanism to identify any covered transactions for which a notice or declaration has not been filed and on which information is reasonably available.

Sec. 10 – Submission of certifications to Congress.
The current CFIUS statute requires CFIUS to submit a certification to Congress upon completion of a review or investigation of a transaction. This section would enhance congressional oversight of the CFIUS process by requiring CFIUS to submit its certifications to both the SSCI and HPSCI (as oversight committees for the U.S. Intelligence Community). It would also provide CFIUS with more flexibility regarding the required signatures on these certifications, easing the current restriction on delegation below the Deputy Secretary level. This section would authorize the chairperson to determine the appropriate level of official to whom the signature requirement may be delegated, and it would allow the delegation to vary based on any appropriate factor relating to a transaction. However, the requirement could not be delegated below the level of Deputy Assistant Secretary (or equivalent). For any transaction that is assessed by the Director of National Intelligence (DNI) as more likely than not to pose a threat to U.S. national security, the requirement could not be delegated below the level of Assistant Secretary (or equivalent). Lastly, this section would authorize CFIUS to "batch" the certifications and send them to Congress on a monthly basis, instead of transmitting them individually.

Sec. 11 – Analysis by Director of National Intelligence.
This section would require the DNI, for each National Security Threat Assessment (NSTA), to:

- Identify any recognized intelligence collection gaps relevant to the NSTA;
- Update the NSTA for any past cleared transaction involving a mitigation agreement, upon request by a lead agency; and
- Submit the NSTA to the SSCI and HPSCI after conclusion of action by CFIUS.

It would authorize the DNI to provide CFIUS, in lieu of full-blown NSTAs, with "Basic Threat Information" (BTI) on any certain transactions, such as those:

- For which the DNI has completed a NSTA involving each foreign investor during the previous 12 months;
- Involving the purchase/lease by a foreign person of U.S. real estate in close proximity to military or other USG national security facilities; and
- Meeting other criteria agreed upon by CFIUS and the DNI.

This section would also require CFIUS to ensure that its processes preserve the independence and objectivity of the DNI in conducting NSTAs and BTIs. Lastly, it would authorize the DNI, for any transaction, to provide CFIUS with a separate assessment of any operational impact of the transaction on the Intelligence Community and a description of any actions being taken to mitigate it.

Sec. 12 – Information sharing.
This section, in conjunction with Sec. 2, would enhance collaboration and coordination with U.S. allies/partners by clarifying that the existing rules on confidentiality do not prohibit the disclosure of:

- Information to any domestic or foreign governmental entity, if necessary for national security (and pursuant to appropriate confidentiality and classification arrangements); or
- Information that the parties have consented to be disclosed to third parties.

Sec. 13 – Action by the President.
This section slightly expands the authority of the President to take action against a transaction to protect national security, giving him/her an additional option (in addition to "suspend or prohibit"). The President would be authorized to "take any additional action" that is appropriate to address national security risks that were identified during the CFIUS review or investigation, thus limiting the possibility of the subsequent evasion of a Presidential suspension or prohibition order. This section also does some statutory housekeeping, confirming that the President's authority includes requiring divestment, when necessary to protect national security. Lastly, for transactions that CFIUS refers to the President for action prior to the

completion of an investigation (see Sec. 18), this section makes a conforming change to the timeline for the President to announce that decision.

Sec. 14 – Judicial review procedures.

The CFIUS statute exempts from judicial review certain actions of the President, including suspension/prohibition of transactions and the making of related findings. This section would extend that exemption to any designee of the President. Additionally, it would create a similar, but more limited, exemption for actions of CFIUS itself, including determinations, recommendations to the President, and various actions related to mitigation agreements or conditions, while also providing a clear process for appeal of CFIUS actions. To resolve uncertainty following the U.S. Court of Appeals for the D.C. Circuit's decision in *Ralls Corp. v. CFIUS*, 758 F.3d 296 (D.C. Cir. 2014), this section would provide that:

- Any party to the transaction may file a petition (within 60 days of the President's/CFIUS' decision), alleging that the action is a violation of a constitutional right, power, privilege, or immunity;
- A party may only file a petition if it previously filed a notice/declaration with CFIUS (or CFIUS determines one was not required), and CFIUS has completed all action;
- The D.C. Circuit has exclusive jurisdiction over any appeal (subject to review by the Supreme Court), and a determination by the court is the exclusive judicial remedy; and
- The court must decide all relevant questions bases solely on an administrative record submitted by the U.S. Govt.

Sec. 15 – Factors to be considered in taking action.

The CFIUS statute lays out 10 specific factors that CFIUS may consider when analyzing a transaction's national security implications. This section would update four of those factors and add nine new ones, providing for consideration of:

- Whether the transaction is likely to have the effect of creating new U.S. cybersecurity vulnerabilities in the U.S. or exacerbating existing ones (new factor);
- The extent to which the transaction is likely to expose personally identifiable information, genetic information, or other sensitive data of U.S. citizens to access by a foreign government/person that may exploit it in a manner that threatens national security (new factor);
- The degree to which the transaction is likely to increase the cost to the U.S. Government of acquiring or maintaining the equipment and systems that are necessary for defense, intelligence, or other national security functions (new factor);
- Whether the transaction involves a country of special concern that has a demonstrated or declared strategic goal of acquiring a type of critical technology that a U.S. business that is a party to the transaction possesses;
- Whether the transaction is likely to reduce the U.S. technological and industrial advantage, relative to any country of special concern (added to existing factor #5);
- Whether the transaction is likely to contribute to the loss of or other adverse effects on technologies that provide the U.S. a strategic national security advantage (added to existing factor #7);
- Whether the transaction is likely to result in increased reliance by the U.S. on foreign suppliers to meet national defense requirements (added to existing factor #1);
- The potential national security-related effects of the cumulative market share of any one type of infrastructure, energy asset, critical material, or critical technology by foreign persons (new factor);
- The potential national security-related effects on transportation assets, as defined in Presidential Policy Directive 21 (added to existing factor #6);
- Whether the foreign investors have a history of complying with U.S. laws/regulations, including those relating to exports, the protection of IP, and immigration, as well as adhering to contracts/agreements with U.S. Govt. entities (new factor);
- Whether the transaction is likely to result in a foreign government gaining a significant new capability to engage in malicious cyber-enabled activities against the U.S., including those designed to affect the outcome of any federal elections (new factor);

- Whether the transaction is likely to facilitate criminal or fraudulent activity affecting U.S. national security; and
- Whether the transaction is likely to expose any information regarding sensitive national security matters or sensitive procedures/operations of a federal law enforcement agency (with national security responsibilities) to an unauthorized foreign entity (new factor).

Sec. 16 – Actions by the Committee to address national security risks.

Suspension or referral of transactions. This section would grant CFIUS the authority to suspend, during a review or investigation, any transaction that may pose a risk to U.S. national security. It would also confirm CFIUS' authority to complete action on a transaction at any point during a review or investigation and refer the transaction to the President for further action against it.

Abandonment of transactions. It would give CFIUS new authority to use mitigation agreements and conditions in situations where the parties have chosen to abandon a transaction, authorizing CFIUS to negotiate, enter into or impose, and enforce any agreement or condition for the purpose of carrying out that abandonment and mitigating any U.S. national security risks that arise. This expressly confirms CFIUS' authority to accept a voluntary abandonment (including through divestment) of a transaction that it has determined poses national security concerns, without needing a public Presidential finding and order.

Interim risk in completed transactions. This section would confirm that CFIUS has the authority to use interim mitigation agreements and conditions regarding completed transactions (that have not yet undergone CFIUS review), authorizing CFIUS to negotiate, enter into or impose, and enforce any agreement or condition until CFIUS has completed action on the transaction or the President has taken action on it, for the purpose of mitigating any interim U.S. national security risks.

Standards for mitigation agreements. It would prohibit CFIUS from entering into any mitigation agreement or imposing any condition regarding a transaction unless CFIUS determines that the agreement/condition resolves any national security concerns posed by the transaction, considering whether it is reasonably calculated to be effective, allows for compliance in an appropriately verifiable way, and enables effective compliance monitoring and enforcement.

Risk-based analysis. This section also requires that a "risk-based analysis" (RBA) of a transaction and its effects on national security be conducted prior to CFIUS referring the transaction to the President for action or suspending the transaction (currently, RBAs are only required before CFIUS pursues a condition or a mitigation agreement). It further requires that the RBA include an assessment of:

- The national security threat posed by the transaction, taking into account the DNI's NSTA;
- Any related national security vulnerabilities; and
- The transaction's potential national security consequences.

It also requires that the RBA include an identification of any national security factors in subsection (f) of the statute (see Sec. 15) that are substantially implicated by the transaction. If any CFIUS member agency concludes that a transaction poses an unresolved national security concern, this section requires that agency to recommend an action and propose the requisite RBA. In the event that CFIUS fails to reach a consensus on a recommendation, it requires the CFIUS member agencies who support an alternative recommendation to produce a written justification for that recommendation and, if needed, an RBA to support it. In so doing, this section provides a clear mechanism through which CFIUS can resolve internal differences over how to handle contentious transactions.

Compliance plans. This section would also require CFIUS to formulate, adhere to, and keep updated a plan for monitoring compliance of cleared transactions involving a mitigation agreement or condition, including:

- Which dept./agency will have primary responsibility for monitoring compliance;
- How compliance will be monitored;
- How frequently compliance reviews will be conducted;

- Whether an independent entity will be utilized to conduct compliance reviews; and
- What action will be taken if the parties fail to cooperate regarding compliance monitoring.

This section also requires CFIUS, if it contracts with an independent entity from outside the U.S. Govt. to conduct compliance monitoring, to take action to prevent a conflict of interest from arising on the part of that independent entity. It would also repeal the current statutory requirement that CFIUS, in developing methods to ensure compliance of mitigation agreements, avoid placing unnecessary burdens on the parties. This section also includes a provision to confirm that U.S. district courts have jurisdiction over actions to enforce and enjoin violations of mitigation agreements, as is already the case with mitigation orders.

Noncompliance. In addition, this section would provide CFIUS with additional tools to use in the event of the parties' noncompliance with mitigation agreements or conditions:

- Negotiating a plan of action for remediating the noncompliance, with failure to abide by the plan serving as a basis for CFIUS to find a material breach;
- Requiring that the parties submit for CFIUS review any new covered transactions for 5 years; and
- Seek injunctive relief.

Sec. 17 – Modification of annual report.

This section would increase transparency by requiring several new elements in each CFIUS annual report:

- A description of the outcomes of any reviews/investigations that year, including whether a mitigation agreement was entered into or condition imposed and whether the President took any action; and
- Statistics on compliance reviews conducted, highlighting any remediation or enforcement actions taken by the Committee.

This section would prohibit the inclusion of any trade secrets or business confidential information in the public version of the annual report. It would also require sharing of the report and its classified annex with eight additional congressional committees that have major equities in the CFIUS process: the SSCI and HPSCI, the SASC and HASC, the Senate Judiciary Committee and House Judiciary Committee, and the Senate HSGAC and House HSC.

In addition, this section would establish a new Intelligence Community (IC) interagency working group on foreign investment risk, led by the DNI, and task it with preparing a biennial report, to be submitted along with the classified annex to the annual CFIUS report in even-numbered years only. The IC report would include identification, analysis, and explanation of:

- Any current or projected major national security threats regarding foreign investment;
- Any strategies used by countries of special concern to utilize foreign investment to target the acquisition of critical technologies, critical materials, or critical infrastructure; and
- Any economic espionage efforts directed at the U.S. by a foreign country, particularly a country of special concern.

Sec. 18 – Certification of notices and information.

Under paragraph (n) of the statute, each notice (and any follow-up information) submitted to CFIUS has to be accompanied by a written statement from the parties, certifying that the notice or information is accurate, complete, and compliant with the rules. This section would prohibit CFIUS from completing a review of any transaction for which such a certification is not submitted, includes false or misleading information, or omits material information. It would also authorize CFIUS, on that basis, to recommend to the President that the transaction be blocked or unwound. Lastly, this section requires CFIUS to prescribe regulations providing for the application of 18 USC 1001, which criminalizes the act of making false statements.

Sec. 19 – Funding.

This section establishes the "CFIUS Fund" and authorizes appropriations ("such sums as may be necessary to perform the functions" of CFIUS). It also authorizes CFIUS to assess and collect filing fees for any

covered transactions for which a notice is filed (but not for declarations). The exact amount would be set by CFIUS in regulations, but it would be capped at 1% of the value of the transaction or $300,000 (indexed for inflation), whichever is lesser. Amounts collected would be deposited into the CFIUS Fund to cover work on reviews, investigations, and other CFIUS activities. They would remain available until expended, and they would be in addition to any appropriations from Congress. Lastly, the chairperson would be authorized to transfer funding from the CFIUS Fund to any member agencies to address emerging needs in executing the requirements of this bill.

Sec. 20 – Centralization of certain Committee functions.
This section would authorize the Secretary of the Treasury (as CFIUS chairperson) to centralize certain CFIUS functions, including monitoring non-notified and non-declared transactions, within the Treasury Dept. to enhance CFIUS interagency coordination and collaboration.

Sec. 21 – Unified budget request.
This section would authorize the President to submit a unified budget request for CFIUS (as a component of his annual budget request for the Dept. of the Treasury), covering any or all CFIUS operations of the CFIUS member agencies and including details and amounts for each dept./agency.

Sec. 22 – Special hiring authority.
This section would authorize CFIUS member agencies to direct-hire candidates for CFIUS jobs, allowing it to bypass certain parts of the traditional hiring process that have made it difficult to identify and hire qualified people in a timely manner. CFIUS work requires individuals who have a specialized skill set, and this change would give CFIUS member agencies the ability to better recruit and hire these individuals in a timely manner, addressing a significant challenge that CFIUS agencies currently face.

Sec. 23 – Conforming amendments.
This section would make six conforming changes to the statute.

Sec. 24 – Assessment of need for additional resources for Committee.
This section would help ensure that CFIUS is fully resourced to carry out its updated statutory mandate, by requiring the President to:

- Determine whether and to what extent the expansion of CFIUS' responsibilities per this legislation necessitates additional resources for CFIUS and its members to perform their functions, and
- Include a request for any such additional resources in his/her annual budget request to Congress.

Sec. 25 – Authorization for DARPA to limit foreign access to technology through contracts and grant agreements.
This section would authorize the DARPA Director, through provisions in contracts or grant agreements, to:

- limit foreign access to technology that is the subject of the contract or grant agreement; and
- if the provision is violated, require the party to return all amounts received from DARPA.

Sec. 26 – Effective date.
This section delays the applicability of some of the bill's most significant provisions until 30 days after the CFIUS chairperson publishes in the Federal Register a determination that the necessary regulations, organizational structure, personnel, and other resources are in place to administer those provisions. However, it makes certain components of the bill effective immediately upon enactment, including certain definitions, requirements, authorities, and reporting requirements. This section also authorizes CFIUS, upon enactment and at its discretion, to conduct pilot programs to implement any authority provided under this bill.

Sec. 27 – Severability.
This section would provide that, if any provision of the bill (or application of the provision) is held to be invalid, the remaining provisions and the application of that provision to other persons shall not be affected.

GROWING SUPPORT FOR FIRRMA

Current U.S. national security leaders back FIRRMA

Secretary of Defense James Mattis (12/15/17 letter):

- "I strongly support the Foreign Investment Risk Review Modernization Act of 2017 (FIRRMA)."
- "DoD depends on critical, foundational, and emerging technologies to maintain military readiness and preserve our technological advantage over potential adversaries. FIRRMA would help close related gaps that exist in both the Committee on Foreign Investment in the United States (CFIUS) and export control processes, which are not presently keeping pace with today's rapid technological changes."
- "CFIUS plays a critical role in protecting the national security of the United States. FIRRMA greatly strengthens that protection and provides much needed CFIUS modernization."

Secretary of the Treasury Steven Mnuchin (quote provided on 12/14/17): "I support the goals of FIRRMA, which will help to ensure that CFIUS has the tools necessary to protect the national security of the United States, while simultaneously maintaining our open investment environment. I stand ready to work with Senators Cornyn, Feinstein, and Burr, the committees of jurisdiction, and other Members of Congress as this important legislation advances."

Attorney General Jeff Sessions (12/13/17 letter): "I am particularly supportive of the goals of several aspects of your proposed legislation, including but not limited to (1) the expansion of CFIUS's authority to review certain transactions that may pose national security concerns; (2) an expanded list of national security factors that CFIUS should consider; and (3) mandatory disclosures of certain investments by state-owned enterprises. . . . I know the Administration stands ready to work with you to enhance our national security."

In addition, on October 18, 2017, at a Senate Judiciary Committee hearing, Attorney General Sessions was asked by Sen. Cornyn whether he supports the effort to modernize and reform the CFIUS process. "I absolutely do. We have looked at that hard in the Department of Justice. I have talked with attorneys and agents who have investigated these cases. They are really worried about our loss of technology. We certainly need additional legislation. Just as you said, you can buy an interest in a company and gain access to the same type of technology. The CFIUS program is not able to be effective enough. Your legislation is first-rate. We think it has great potential to push back against the abuses and dangers we face. I'm excited about it, and anything I can do to say, publicly, thank you for that work and to call on Congress to move on it rapidly. You would be winning the confidence and support of people who investigate these matters every day and know what's going on. They support what you're doing, and I hope Congress can follow through."

Admiral Harry Harris, U.S. Navy, Commander of U.S. Pacific Command (1/3/18 letter):
"Within the USPACOM area of responsibility, China represents our greatest long-term security challenge. China blurs the lines between military and civilian activity and uses its state-owned and private enterprises to exploit our open system and gain access to U.S. civil, military, and dual-use technologies. China leverages these technologies to strengthen its comprehensive national power. It is emboldened to coerce its neighbors and violate international norms and standards. This puts at risk our regional and global military advantage and influence, and ultimately our security and prosperity. Through the Department of Defense's participation in the CFIUS process, we are well aware that CFIUS is protecting America's crown jewels – our advanced technologies. I strongly support strengthening the CFIUS process via FIRRMA."

Former U.S. national security leaders back FIRRMA

Former Secretary of Defense Donald Rumsfeld (1/12/18 letter):

- "This letter is to express my support for the Foreign Investment Risk Review Modernization Act (FIRRMA). China's rise has produced a set of unprecedented, anti-free-market policies through which it is able to aggressively absorb advanced U.S. technology and know-how to fuel its continuing military modernization. In a relatively short period, China has become an industrial and technological challenge, thanks to both its illicit and licit activities, such as foreign investment and transfers of technology and know-how from U.S. companies."
- "In addition to serving twice as Secretary of Defense, I have also led corporations in the fields of pharmaceuticals and electronics, as well as served as a board member on other companies. As I understand it, FIRRMA would take a targeted and responsible approach to a set of complex issues. Under its provisions, the CFIUS process and the export control system would remain complementary. These systems need to be interoperable in order to begin to effectively address the full range of mounting national security issues regarding China's activities. FIRRMA would represent an important step towards modernizing our policies for the 21st Century. We must be clear-eyed about the implications of the transfer of industrial capabilities and we must do more than stand by and watch as China's actions challenge our national security edge."

Former Secretary of Homeland Secretary Michael Chertoff (quote provided on 12/27/17): "The bipartisan Foreign Investment Risk Review Modernization Act (FIRRMA) is a long overdue and welcome modernization of our CFIUS foreign investment review process. The Act plugs loopholes in our national security reviews, and adopts a holistic, risk-based analytic approach in evaluating foreign investments. FIRRMA recognizes the value of foreign investment in the United States, but assures that we can protect our key security technologies and interests from theft or manipulation."

Former Secretary of Defense Bill Perry (12/18/17 letter):

- "I write to express my strong support for your bipartisan legislation, the Foreign Investment Risk Review Modernization Act of 2017 (FIRRMA)."
- "China has identified gaps in the CFIUS process and export control system and is exploiting them to acquire industrial capabilities in dual-use U.S. technologies, aiding its own military modernization and weakening our U.S. defense industrial base. FIRRMA takes a measured and targeted approach to close these gaps, with reforms that are laser-focused on national security concerns."
- "In the interests of national security, I urge the enactment of this critical legislation as soon as possible."

Admiral Dennis Blair, U.S. Navy (retired), former Director of National Intelligence and Commander of U.S. Pacific Command (quote provided on 11/21/17): "As co-chair of the Commission on the Theft of American Intellectual Property, I welcome the much-needed CFIUS reforms provided in the Foreign Investment Risk Review Modernization Act (FIRRMA), especially with regard to the inclusion of IP protection as a factor to be considered in the CFIUS review process. The IP Commission has long argued for this provision. By expanding the scope of CFIUS reviews, FIRRMA provides better tools to analyze foreign investments and thus will strengthen the protection of America intellectual property from theft by foreign actors."

Admiral William H. McRaven, U.S. Navy (retired), former Commander of U.S. Special Operations Command (quote provided on 1/17/18): "As a free market nation we should continue to encourage foreign investment in U.S. companies and the expansion of our global marketplace, all the while remaining attentive to our national security. I believe that modernizing the CFIUS process will balance these concerns, and that FIRRMA is a good move toward accomplishing this."

General Mark Welsh, USAF (retired), former U.S. Air Force Chief of Staff (quote provided on 1/17/18): "Finding the balance between engaging in an active, integrated global marketplace and ensuring national security, is a difficult, but critically important task for our nation's leaders. I believe FIRRMA would give them an important new tool to help preserve that delicate balance."

General Mike Hagee, USMC (retired), former U.S. Marine Corps Commandant (12/21/17 letter):

- "China continues its aggressive campaign to use both licit and illicit means to acquire and absorb advanced U.S. technology and know-how to fuel its rapid military modernization, and we must be clear-eyed about the implications for our long-term national security."
- "CFIUS plays a critical role, as does the export control system, but neither have proven able to adequately address the range of national security risks inherent in Chinese investment in the U.S."
- "In the interests of national security, I urge the enactment of this critical legislation as soon as possible."

General Edward Rice, USAF (retired), former Vice Commander of Pacific Air Forces and Commander of U.S. Forces in Japan (12/29/17 letter):

- "I write to express my strong support for your bipartisan legislation, the Foreign Investment Risk Review Modernization Act of 2017 (FIRRMA)."
- "In this regard, the PRC [People's Republic of China] has a long history of accelerating its military development through the acquisition and integration of U.S. technology by legitimate and illegitimate means."
- "In my judgement, FIRRMA strikes the right balance between harvesting the benefits of foreign investment in the United States and safeguarding technologies that are critical to our national security interests."

General J.D. Thurman, U.S. Army (retired), former Commander of U.S. Forces Korea and U.S. Army Forces Command (12/21/17 letter):

- "In particular, China's investment activities are contributing to a marked shift in the strategic balance between our countries and eroding the overall U.S. military advantage over potential adversaries that has underpinned our own national security and economic prosperity since the end of World War II."
- "China has identified gaps in the CFIUS process and export control system and is exploiting them to acquire industrial capabilities in dual-use U.S technologies, aiding its own military modernization and weakening our U.S. defense industrial base. FIRRMA takes a measured and targeted approach to close these gaps, with reforms that are laser-focused on national security concerns."
- "In the interests of national security, I urge the enactment of this critical legislation as soon as possible."

Private industry players back FIRRMA

Ericsson, Inc. (1/16/18 letter):

- "[W]e commend you . . . for spearheading the Foreign Investment Risk Review Modernization Act (FIRRMA). This legislation provides critical and overdue updates to the Committee of Foreign Investment in the United States (CFIUS) review process."
- "And we must ensure there are adequate safeguards in place to property vet and scrutinize the efforts by foreign entities to gain access to our markets, and our technology. In short, FIRRMA helps provide that assurance by arming CFIUS with the tools necessary to preserve our national security interests while not discouraging investment in the United States. It's an important effort

in a regulatory area that requires modernization, without which will result in the potential compromise of technology developed by companies like Ericsson and in turn, our national security."

Oracle Corporation (11/8/17 letter):

- "This important legislation will modernize and update the process used by the Committee on Foreign Investment in the United States (CFIUS) to conduct reviews of transactions that could result in a foreign entity gaining access to critical technologies and related know-how, reducing the U.S. technological and military advantage over potential adversaries."
- "The current CFIUS process does not fully take into consideration evolving strategies used to bypass attempts to acquire control of American businesses in favor of alternative mechanisms to obtain access to leading edge technology via smaller investments or joint ventures. Without reform, CFIUS will fail to address the use of these techniques that circumvent an essential review process, putting at risk critical innovations that bolster and ensure our national security."

Trinity Industries (1/17/18 letter): "S.2098 will expand the federal government's authority to review foreign purchases of and minority investments in U.S. firms by strengthening the Committee on Foreign Investment in the United States (CFIUS) process. This important legislation will modernize the ability of CFIUS to conduct reviews of transactions that could result in a foreign entity gaining access to critical technologies and critical infrastructure that may threaten our national security. . . . Trinity agrees with the need to reform and expand the CFIUS process as set forth in FIRRMA."

Amsted Rail Company, Inc. (1/16/18 letter): "This important legislation will modernize the ability of CFIUS to conduct reviews of transactions that could result in a foreign entity gaining access to critical technologies and our nation's critical infrastructure. . . . FIRRMA strikes a balance of protecting national security while not chilling the benefits of foreign investment in the United States. Amsted Rail agrees with the need to reform and expand the CFIUS process as set forth in FIRRMA."

The Greenbrier Companies (1/16/18 letter): "This important legislation will modernize the ability of CFIUS to conduct reviews of transactions that could result in a foreign entity gaining access to critical technologies and our nation's critical infrastructure. . . . FIRRMA strikes a balance of protecting national security while not chilling the benefits of foreign investment in the United States. Greenbrier agrees with the need to reform and expand the CFIUS process as set forth in FIRRMA."

American Iron and Steel Institute (20 member companies) (1/17/18 letter): "In our view, the current CFIUS review process is in need of updating. Over time, foreign adversaries have found ways to circumvent the existing review process, in the process threatening our national security. By requiring mandatory filings for investments by state-owned enterprises, adding new national security factors for CFIUS to consider, and updating the definition of 'critical technologies,' this legislation enhances our national security without discouraging foreign investments that benefit the U.S. economy. AISI agrees with the need to modernize the CFIUS review process and we believe this legislation will accomplish this important goal."

Railway Supply Institute (11/15/17 letter):

- "This important legislation will help to modernize and update the process used by CFIUS to conduct reviews of transactions that could result in a foreign entity gaining access to critical technologies and potentially our nation's critical infrastructure."
- "RSI represents over 260 companies and acts on behalf of the largest and smallest suppliers to North American freight and passenger railroads."
- "RSI agrees with the need to reform and expand the CFIUS process as set forth in FIRRMA and we thank you for your attention to this issue and introduction of this important legislation."

China expert backs FIRRMA

Dr. Larry M. Wortzel, Commissioner, U.S.-China Economic and Security Review Commission (quote provided on 10/25/17):

- "The Committee of Foreign Investment in the United States (CFIUS) was created in a time of substantially less foreign investment and to address challenges which have increased in complexity and sophistication in the last decade. Today, United States security is challenged in particular by a determined, centrally controlled effort by China to acquire the most advanced U.S. technology and to acquire large segments of our economy and industry. Senator Cornyn's Foreign Investment Risk Review Modernization Act updates the law to better protect U.S. national security assets and close loopholes in the existing statute."
- "Innovation is an important driver of U.S. economic prosperity, and U.S. laws must keep pace with a rapidly evolving tech landscape. Senator Cornyn's Foreign Investment Risk Review Modernization Act helps prepare the United States to meet these new challenges and mitigate risks posed by current and emerging security threats."

Other support from current U.S. national security leaders for CFIUS modernization

The Trump Administration's National Security Strategy (December 2017): "While maintaining an investor-friendly climate, this Administration will work with the Congress to strengthen the Committee on Foreign Investment in the United States (CFIUS) to ensure it addresses current and future national security risks."

Secretary of Defense Jim Mattis, at a Senate Armed Services Committee (SASC) hearing on June 13, 2017, also testified that "rapid technological change" is one of several concurrent forces acting on the Defense Department, and it includes "developments in advanced computing, big data analytics, artificial intelligence, autonomy, robotics, miniaturization, additive manufacturing, meta-materials, directed energy, and hypersonics – the very technologies that ensure we will be able to fight and win the wars of the future." He recognized that many of these advances are driven by the commercial sector, and that "new commercial technologies will change society, and ultimately, they will change the character of war." When asked by Sen. Gary Peters (D-MI) whether there is "a national security benefit to taking a tougher line against certain types of investment from nations that pose a clear threat to our national security, like China," Sec. Mattis replied, "Absolutely there is. I completely agree with your view that CFIUS is outdated, sir, and needs to be updated to deal with today's situation." **USMC Gen. Joe Dunford, Chairman of the Joint Chiefs of Staff**, voiced strong agreement.

At a Senate Select Committee on Intelligence open hearing on May 12, 2017, several senior Intelligence Community officials, when asked by Sen. Cornyn whether the current CFIUS process is adequate, expressed support for the idea of CFIUS reform.

- **Dan Coats, Director of National Intelligence**, said "I certainly think that, given China's aggressive approach relative to information gathering and all the things that you mentioned merits a review of CFIUS in terms of whether or not it is -- needs to have some changes or innovations to address the aggressive Chinese actions not just against our companies, but across the world."
- **Mike Pompeo, Director of the CIA**, said that CFIUS "mostly deals with changing control transactions, purchases. There are many other ways one could invest in an entity here in the United States and exert significant control over that entity, I think that ought to be looked at."

DNI Coats, at a SASC hearing on May 23, 2017, said "we ought to do a significant review of the current CFIUS situation to bring it up to speed . . . ."

Admiral Michael Rogers, Director of the NSA (and Commander of U.S. Cyber Command), said at a SASC hearing on May 9, 2017: "I think we need to step back and reassess the CFIUS process and make sure it's optimized for the world of today and tomorrow, because I'm watching nation-states generate insight and knowledge about our processes. They understand our CFIUS structure. They understand the criteria, broadly, that we use to make broader policy decisions about, is an investment acceptable from a national security perspective. And my concern is -- you're watching some nation-states change their methodology to -- to try to get around this process."

Steven Mnuchin, Secretary of the Treasury, at a House Financial Services Committee hearing on July 27, 2017, also said this about CFIUS reform: "There are some obvious changes we need to make to CFIUS – one of which is CFIUS doesn't cover joint ventures. But as we've had the opportunity to talk about, and we look forward to working with you and others, there's a laundry list of changes that we look forward to making with you." When asked whether he agreed that this issue is pressing, he agreed that it is.

Wilbur Ross, Secretary of Commerce, at a public forum on June 12, 2017, said: "Where I think CFIUS is weak – and there's a lot of talk within the administration about trying to build it up – it doesn't deal with joint ventures and it really tends to focus more on big companies. But to me one of the real dangers is not the giant companies, but two young kids in a garage somewhere that are onto some new technology, and [CFIUS] isn't very well set up to deal with that."

STATEMENT FOR THE RECORD OF

THE RAIL SECURITY ALLIANCE

BEFORE THE

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

AT A HEARING ENTITLED

"CFIUS REFORM: EXAMINING THE ESSENTIAL ELEMENTS"

JANUARY 18, 2018

1341 G St. NW 6th Floor| Washington, DC 20005 | 202. 466. 5053

Introduction

The Rail Security Alliance (RSA), a collaborative of American freight rail manufacturers, suppliers and other interests, appreciates the opportunity to submit a statement for the record to the Senate Committee on Banking, Housing, and Urban Affairs to highlight the urgent need for reforms to the Committee on Foreign Investment in the United States (CFIUS). As the Committee is aware, CFIUS has long served as an important tool for protecting U.S. national security interests from being compromised by foreign investments. However, the evolution of digital technologies, increased use of murky financing by foreign investors, and a changing international landscape since the last CFIUS update in 2007, among other things, suggest that the CFIUS is very much in need of an overhaul, as it is often ill-equipped to deal with these new risks to economic and national security.

Chinese state-owned enterprises have particularly, and troublingly, exploited these gaps in the CFIUS process to strategically entrench Chinese government-owned firms in the American freight rail manufacturing sector among other industries across the United States. Allowing China to continue to target and do harm to the stability of U.S. freight rail manufacturing not only threatens roughly 65,000 American jobs,[1] but also has the potential to severely compromise our economic and national security.

Freight rail is a core component of U.S. critical infrastructure, according to the Department of Homeland Security.[2] With nearly 140,000 miles of railroad covering the United States, freight rail regularly transports sensitive materials such as oil and nuclear waste that are integral to American defense and economic infrastructure. Yet freight manufacturing, which offers Chinese interests an opportunity to offload excess capacity of both freight supplies as well as steel and other raw materials, has increasingly drawn Chinese government investment activity in the United States. Today, Chinese state-owned interests are using circuitous and anti-competitive tactics to build freight rail manufacturing capabilities in the U.S. market that are undermining U.S. industry and raising dire concerns about the national and economic security of the United States. Despite the intent of Congress when it first established CFIUS over 40 years ago, the CFIUS process as we know it is not equipped to address these urgent challenges.

As Congress examines possible reforms to CFIUS to address these gaps, we ask the Committee to consider these critical facts:

- China is strategically targeting the U.S. freight rail manufacturing sector, first with aggressive and anticompetitive early moves into U.S. transit rail that have nabbed four

[1] Oxford Economics, *Will We Derail US Freight Rolling Stock Production?*, May 2017, at 5.
[2] Department of Homeland Security, *Transportation Systems Sector Overview,* July 6, 2017. https://www.dhs.gov/transportation-systems-sector

U.S. metropolitan transit contracts thus far, largely through anticompetitive underbidding practices.

- With China's government picking up U.S. transit rail contracts, Chinese state-owned enterprises are now using their rail manufacturing capabilities to take on the U.S. freight manufacturing sector.

- This activity is a pattern for China's state-owned rail sector: Over the last nine years, it has systematically wiped out the entire freight rail manufacturing capability in Australia. Without proper government oversight, the same thing could all-too-easily occur in the U.S. market.

- The upshot of such a catastrophe would be felt not only by the U.S. manufacturing sector: Forcing America's industrial, military, and other government interests to rely significantly or wholly on Chinese government-made freight rail cars raises grave security concerns.

- CFIUS has thus far failed to recognize these concerns or been able to address the implications of having the Chinese government closely involved in a core sector of our nation's infrastructure.

- According to the National Security Council, the Chinese are targeting 13 additional industries aside from freight rail across the United States where primary motivation is market share and profit-making comes second, if at all.

China's CRRC Targets U.S. Rail Manufacturing

The "Made in China 2025" initiative, a key component of China's 13th Five-Year plan,[3] identifies the rail manufacturing sector as a top target for Chinese expansion and has driven strategic investment and financing activities of the China Railroad Rolling Stock Corporation (CRRC) in third-country markets and the United States. CRRC is wholly owned by the Government of China and it has 90 percent of China's domestic market for production of rail locomotives, bullet trains, passenger trains and metro vehicles.[4] In 2015, CRRC reported revenues of more than $37 billion[4] — significantly outpacing the entire U.S. railcar market, which had $22 billion of output during the same year.[5] According to Chinese state media, CRRC

[3] U.S.-China Economic and Security Review Commission, *2016 Report to Congress*, November 2016, at 100. [4] Langi Chiang, *China's largest train maker CRRC Corp announces 12.2 billion yuan in contracts*, South China Morning REPORT, July 23, 2015.
[4] Macquarie Research, *CRRC Corp Ltd: Too big to roll too fast*, May 20, 2016, at 3.
[5] Oxford Economics, *Will We Derail US Freight Rolling Stock Production?*, May 2017, at 24.

plans to increase overseas sales to $15 billion by 2020, about double the level of export orders in 2014,[6] and the U.S. market is a prime target.

Since 2015, we have witnessed CRRC establish rail assembly operations in three states, along with additional research and bidding operations in three others. By beginning with a business strategy to take market share in the U.S. transit rail manufacturing sector and deploying near-limitless financing from its home government to help lower the below-market bids for new U.S. metropolitan transit projects, CRRC has quickly established itself as an unbeatable force in U.S. transit rail competition.

Several recent cases involving CRRC bids for new transit rail projects serve as compelling examples:

- CRRC bid $567 million – roughly half the next highest bid (from Bombardier, a company with a longstanding U.S. manufacturing workforce and footprint) – to win the contract with the MBTA in Boston in 2014.[7] The initial order of fully-built, in China, CRRC railcars were delivered to Boston late last year.

- In 2016, CRRC won a contract to provide transit rail for the Chicago's CTA, bidding $226 million less than the next-highest bidder.[89]

- In early 2017, CRRC bid $137.5 million for a contract with SEPTA in Philadelphia, underbidding the next-largest bidder by $34 million.[10]

- In March 2017, CRRC finalized a contract with the Los Angeles County Metropolitan Transportation Authority for its transit rail system that could be worth up to $647 million,[11] reportedly leveraging below-market financing to enable them to undercut other bidders.

Faced with the outcomes of these anticompetitive tactics, transit rail manufacturers in the U.S. market are feeling the pinch and many have already begun to downsize U.S. manufacturing

---

[6] Brenda Goh, *China Trainmaker CRRC to build more plants abroad in expansion plan: China Daily*, REUTERS, Dec. 5, 2016, http://www.reuters.com/article/us-crrc-expansion-idUSKBN13U0EJ.

[7] Bonnie Cao, *After Winning MBTA Contract, China Trainmaker CRRC Plans American Expansion*, Boston Globe, Sept. 11, 2015. https://www.bostonglobe.com/business/2015/09/11/after-winning-mbta-contract-china-trainmakercrrc-plans-american-expansion/jnS1kU7uHWFGR9giWmDEjM/story.html

[8] Corilyn Shropshire, *First Step to New CTA Rail Cars: Build the Factory in Chicago*, Chicago Tribune, Mar. 16,

[9] , http://www.chicagotribune.com/business/ct-cta-new-railcar-plant-0316-biz-20170315-story.html

[10] Jason Laughlin, *Mass.-Based Company with Chinese Backing Beats Local Group for SEPTA Car Contract*, The Philadelphia Inquirer, Mar. 21, 2017. http://www.philly.com/philly/business/transportation/Mass-based-companywith-Chinese-backing-beats-out-local-group-for-SEPTA-car-contract.html

[11] Keith Barrow, *Los Angeles Orders CRRC Metro Cars*, International Railway Journal, Mar. 24, 2017. http://www.railjournal.com/index.php/north-america/los-angeles-orders-crrc-metro-cars.html

facilities and workforces,[12][13] with the prospects of more workforce reductions to come. Anticipating the opportunity to unseat other manufacturers here and take advantage of the opportunity that these U.S. job reductions are likely to create, CRRC most recently announced that it is developing a 204,000-square foot plant in Springfield, Massachusetts, where it will assemble railcar components shipped from China to the United States.[14]

The dangers to allowing CRRC's anticompetitive actions are evident in Australia, whose rail manufacturing sector CRRC entered in 2008. In less than 10 years, CRRC effectively decimated the sector, undoing the other four manufacturers in that country, which left only CRRC standing.[15] CRRC leveraged financing from its own government to help customers acquire its product at costs well below the market. Today, almost no meaningful Australian freight rolling stock manufacturing exists[16] – CRRC's Australia footprint is almost exclusively that of an assembler of Chinese-made parts and a financier of purchases from CRRC.

CRRC: A Case Study for CFIUS Reform

In 2016, CRRC announced a joint venture with Majestic Legend Holdings Limited and Vertex Rail Technology to create a new railcar manufacturing enterprise, Vertex Rail Corporation. This initial formation appeared to be structured as a greenfield investment, avoiding a CFIUS review, though this is mostly optical, as the company is effectively a way to enable the Chinese government investment in a subsidiary of Vertex Rail Technology. Public reports from Vertex's general counsel indicated that ownership would transfer once the company produced several hundred freight cars. Due to this alarming investment by the Chinese government, 55 Members of the House and 42 Senators raised concerns about this transaction and urged CFIUS to investigate.[17] Nevertheless, Vertex announced in late 2016 that CFIUS would allow the deal to move forward. Given CRRC's existing stronghold in U.S. transit rail, the Vertex deal now provides CRRC with the opportunity to rapidly expand into the freight rail sector where additional national security risks come into play.

Implications for National Security

Unlike the U.S. maritime shipping industry, whose security is protected by the 100-year-old Jones Act – a measure that requires vessels transporting goods between U.S. ports to be U.S. built and majority U.S.-owned – freight rail in America has been left comparatively unprotected.

---

[12] See *UPDATE: GE closing 3 former Alstom plants in Chattanooga*, WRCB, June 21,

[13] ,http://www.wrcbtv.com/story/32156061/update-ge-closing-3-former-alstom-plants-in-chattanooga; *GE making layoffs at Salem plant*," WDBJ7, Mar. 24, 2017, http://www.wdbj7.com/content/news/GE-making-layoffs-at-Salemplant-417044683.html

[14] Jim Kinney, *CRRC MA Springfield plant has deal to build subway cars for Los Angeles*, MASSLIVE, Dec. 22, 2016, http://www.masslive.com/business-news/index.ssf/2016/12/crrc_plans_final_assembly_of_los_angeles.html.

[15] *Id.*

[16] *Id.* at 15-16.

[17] Brandon Wissbaum, *Congress members call for investigation into Vertex's ties with Chinese corporations, WECT, July 29, 2016. http://www.wect.com/story/32574814/congress-members-call-for-investigation-into-vertexs-ties-with-chinese-corporations*

Yet the Department of Homeland Security (DHS) deems the U.S. rail sector as part of the nation's critical infrastructure,[18] noting that 140,000 rail miles enable U.S. freight rail to run through every major American city and every military base in the nation. Freight rail transports not only military freight and industrial products, but also nuclear material and hazardous chemicals that can be safely and effectively transported only by rail. There are very real concerns, DHS has noted, about freight rail vulnerability, including through cyber-attack. As DHS reported in 2010:

> *With the merger of information system technology and transportation infrastructure, railroad operations have become increasingly reliant on information systems and communications technologies. Rail companies have made growing use of onboard-computers, local area networks, automated equipment identifiers, global positioning system (GPS) tracking, automatic reporting of work orders to headquarters, car scheduling and train order systems, and two-way wireless communications. . .. Nearly all . . . rail cars are tagged with automatic identification transponders, which automatically record and report car location as it passes a wayside detector. . .. The railroad's growing dependence on these centralized monitoring and control systems, including Centralized Traffic Control networks, prompts concerns of possible cyber-attacks upon these systems.*[19]

That assessment, written seven years ago, did not account for substantially more complex digital capabilities that have since evolved, or are in development, for U.S. freight rail cars and freight train operations. Yet, the assessment underscores the clear danger of a foreign country, and particularly the government of China and its state-owned enterprises, having undue control of freight manufacturing in the U.S. market.

Already, there are reports of Chinese manufacturers investigating the production of their own "telematics" technology to allow the monitoring and control of their freight cars.[20] Needless to say, as China's CRRC becomes more dominant as a U.S. rail manufacturer, there are urgent questions we must answer regarding whether a growing presence of – and reliance on –freight cars from the major state-owned Chinese rail enterprise could compromise the security and safety of industrial, military, and other U.S. freight shipments.

---

[18] Presidential Policy Directive 21 (PPD-21) identifies 16 critical infrastructure sectors, including "Transportation Systems." The Department of Homeland Security defines "Freight Rail" as one of the seven key subsectors. *See generally*, PPD-21, *Critical Infrastructure Security and Resilience*, Feb. 12, 2013, https://www.whitehouse.gov/thepress-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil and *Transportation Systems Sector*, Dep't of Homeland Sec., Mar. 25, 2013, http://www.dhs.gov/transportation-systems-sector.

[19] Department of Homeland Security, Transportation Systems Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan (2010), at 285.

[20] *China plans 'smart trains' to take on global rail companies*, CHINA DAILY, March 10, 2016, http://english.chinamil.com.cn/news-channels/2016-03/10/content_6952271_2.htm.

Recommendations

This hearing is an important step to amending CFIUS to enable the U.S. Government to tackle this pressing challenge. As Congress debates this issue, we recommend the following updates be made to CFIUS:

- Expand the Committee's jurisdiction to cover greenfield investments where an investor is a foreign sovereign, state owned enterprise or is financed by such a party.
- Expanded definition of "control by a foreign government" to include the access of the buyer to below-market loans and other financing directly or indirectly from government sources.
- Systematically increased scrutiny of investments from certain countries, like China, that pose a significant threat to the United States or have demonstrated a strategic goal of investing in U.S. manufacturing or critical infrastructure sectors.
- Expand existing factors of consideration in the CFIUS process to include patterns of investment and their potential long-term effects on market share in a critical infrastructure sector.
- Ensure mandatory reviews of foreign investments by a state-owned enterprise in any U.S. critical infrastructure sector.

Conclusion

We appreciate the Committee's interest in addressing these issues. The strategic targeting of our nation's infrastructure by the government of China and its state-owned enterprises poses a fundamental threat not only to the economic and security of the United States, but to our country's standing as a global power. Addressing these concerns will not follow any single solution, but we believe reforms to the CFIUS process are an essential part of protecting U.S. infrastructure from being compromised by foreign influence. To that end, we support efforts being led by Senator Cornyn to pursue needed changes to the CFIUS law, as well as other similar efforts to bolster the Administration's ability to track and protect U.S. economic interests relative to investment activity by SOEs in the rail manufacturing sector.

Thank you again for the opportunity to submit testimony and the members of RSA look forward to hearing the solutions put forward by Congress to address these threats.

Respectfully submitted,

Erik Robert Olson
Vice President

1341 G St. NW 6th Floor| Washington, DC 20005 | 202. 466. 5053