EXAMINING THE OPERATIONS OF THE COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES (CFIUS)

HEARING

BEFORE THE

SUBCOMMITTEE ON MONETARY POLICY AND TRADE

OF THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

DECEMBER 14, 2017

Printed for the use of the Committee on Financial Services

Serial No. 115–66

U.S. GOVERNMENT PUBLISHING OFFICE

31–297 PDF WASHINGTON : 2018

HOUSE COMMITTEE ON FINANCIAL SERVICES

JEB HENSARLING, Texas, *Chairman*

PATRICK T. McHENRY, North Carolina, *Vice Chairman*
PETER T. KING, New York
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
STEVAN PEARCE, New Mexico
BILL POSEY, Florida
BLAINE LUETKEMEYER, Missouri
BILL HUIZENGA, Michigan
SEAN P. DUFFY, Wisconsin
STEVE STIVERS, Ohio
RANDY HULTGREN, Illinois
DENNIS A. ROSS, Florida
ROBERT PITTENGER, North Carolina
ANN WAGNER, Missouri
ANDY BARR, Kentucky
KEITH J. ROTHFUS, Pennsylvania
LUKE MESSER, Indiana
SCOTT TIPTON, Colorado
ROGER WILLIAMS, Texas
BRUCE POLIQUIN, Maine
MIA LOVE, Utah
FRENCH HILL, Arkansas
TOM EMMER, Minnesota
LEE M. ZELDIN, New York
DAVID A. TROTT, Michigan
BARRY LOUDERMILK, Georgia
ALEXANDER X. MOONEY, West Virginia
THOMAS MacARTHUR, New Jersey
WARREN DAVIDSON, Ohio
TED BUDD, North Carolina
DAVID KUSTOFF, Tennessee
CLAUDIA TENNEY, New York
TREY HOLLINGSWORTH, Indiana

MAXINE WATERS, California, *Ranking Member*
CAROLYN B. MALONEY, New York
NYDIA M. VELÁZQUEZ, New York
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
MICHAEL E. CAPUANO, Massachusetts
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
DAVID SCOTT, Georgia
AL GREEN, Texas
EMANUEL CLEAVER, Missouri
GWEN MOORE, Wisconsin
KEITH ELLISON, Minnesota
ED PERLMUTTER, Colorado
JAMES A. HIMES, Connecticut
BILL FOSTER, Illinois
DANIEL T. KILDEE, Michigan
JOHN K. DELANEY, Maryland
KYRSTEN SINEMA, Arizona
JOYCE BEATTY, Ohio
DENNY HECK, Washington
JUAN VARGAS, California
JOSH GOTTHEIMER, New Jersey
VICENTE GONZALEZ, Texas
CHARLIE CRIST, Florida
RUBEN KIHUEN, Nevada

KIRSTEN SUTTON MORK, *Staff Director*

SUBCOMMITTEE ON MONETARY POLICY AND TRADE

ANDY BARR, Kentucky, *Chairman*

ROGER WILLIAMS, Texas, *Vice Chairman*
FRANK D. LUCAS, Oklahoma
BILL HUIZENGA, Michigan
ROBERT PITTENGER, North Carolina
MIA LOVE, Utah
FRENCH HILL, Arkansas
TOM EMMER, Minnesota
ALEXANDER X. MOONEY, West Virginia
WARREN DAVIDSON, Ohio
CLAUDIA TENNEY, New York
TREY HOLLINGSWORTH, Indiana

GWEN MOORE, Wisconsin, *Ranking Member*
GREGORY W. MEEKS, New York
BILL FOSTER, Illinois
BRAD SHERMAN, California
AL GREEN, Texas
DENNY HECK, Washington
DANIEL T. KILDEE, Michigan
JUAN VARGAS, California
CHARLIE CRIST, Florida

CONTENTS

WITNESSES

THURSDAY, DECEMBER 14, 2017

APPENDIX

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

EXAMINING THE OPERATIONS OF THE COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES (CFIUS)

Thursday, December 14, 2017

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON MONETARY POLICY AND TRADE,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The subcommittee met, pursuant to notice, at 9:09 a.m., in room 2128, Rayburn House Office Building, Hon. Andy Barr [chairman of the subcommittee] presiding.

Present: Representatives Barr, Lucas, Huizenga, Pittenger, Love, Hill, Emmer, Mooney, Davidson, Tenney, Hollingsworth, Foster, Sherman, Green, Heck, and Crist.

Chairman BARR. The committee will come to order.

Without objection, the Chair is authorized to declare a recess of the committee at any time, and all members will have 5 legislative days within which to submit extraneous materials to the Chair for inclusion in the record. This hearing is entitled "Examining the Operations of the Committee on Foreign Investment in the United States." I now recognize myself for 5 minutes to give an opening statement.

The free flow of capital is a bedrock tenet of the United States economy, ensuring that free flow worldwide has always been a bipartisan goal. And, to that end, I am proud to serve as Co-chair of the Global Investment in America Caucus, along with our colleagues Mr. Holding, Mr. Himes, and Mr. Meeks. The caucus promotes global investment in the United States economy, and helps educate members about the importance of foreign direct investment. Today, the United States is both the largest foreign investor, and the recipient of the greatest amount of foreign direct investment.

That capital has provided a good deal of the energy that has kept our economy vibrant, compensating, to some extent, for our notoriously low national savings rate to provide the fuel for growth of U.S. businesses and jobs. Today, almost 5 percent of U.S. workers and jobs are related to foreign investment. Most of these jobs pay handsomely, far better, on average, than other U.S. jobs. But, if foreign investment is to be a force for good, it must not be welcomed unthinkingly any more than one might leave the front door of a house open around the clock. Investment that might weaken us is not good or welcome investment, and we must guard against it. That investment might come for purely economic reasons. But

especially in this era of international turmoil, conflict, and economic uncertainty, it can also come from individuals or nation-states that might wish to weaken our economy in comparison to theirs, or try to spirit away technology or know-how that could strengthen their military to gain an advantage over ours.

To maintain a vigilant watch on investment, the multi-agency Committee on Foreign Investment in the United States, or CFIUS, reviews many inbound investments to determine if they pose a threat to national security. This involves rigorous scrutiny of proposals by all appropriate departments or agencies, including a scrub by the intelligence community. And the President has the power to block transactions, or order divestments, if such concerns cannot be mitigated by a change in the original proposal.

Today, we face new threats on a number of fronts, not just the threat of a hollowed-out industrial sector, but also from terrorism and from major nations that are economic competitors, but also potential military competitors. I am referring, of course, mainly, to China. Concerns have risen sharply in the past years about Chinese companies using that country's vast financial reserves to acquire key technology with an eye toward taking the lead in the industrial markets of the future. The Chinese Government, for example, has set aside $250 billion to be used in dominating the vital semiconductor market. This is not a new phenomenon, but just a new challenger.

President Ford set up CFIUS in 1975 out of concern that the vast inflows coming from OPEC countries could weaken our economy. In 1988, among concerns that Japan was seeking to buy critical technology, Congress gave President Reagan the authority to actually block deals. That authority only has been used sparingly. Interestingly, the first use came when President George H.W. Bush blocked the sale of an airplane component maker to a Chinese company.

More recently, President Obama, just before he left office, blocked a Chinese deal, and President Trump already has blocked the proposed purchase of lattice semiconductors by a Chinese company.

CFIUS has also approved foreign direct investment conditionally, approving a deal only when divestment of divisions with sensitive technologies or activities has occurred. But the statute under which CFIUS operates has not been updated in a decade, and, clearly, we should think about modernizing it. Aside from China's intentions, there are burdens on the CFIUS process from the volume and complexity of proposed deals. There were about 40 percent more reviews in 2017 than 2016, and a more than fourfold expansion in the number of Chinese-backed deals just since 2013.

To that end, our colleague, Representative Pittenger and Senator Cornyn, have spent more than a year studying the CFIUS process and considering possible reforms. I commend their work.

This hearing is the beginning of the committee's study of CFIUS and will be followed by further hearings soon. In considering any reforms, the committee will seek to ensure that CFIUS has the tools and resources it needs to examine foreign investment. As Members of Congress, it is our duty to advance the national security of the United States. At the same time, we must aspire, to the

greatest extent possible, a welcoming investment climate so that U.S. companies have the capital needed to grow. As well, we need to be mindful that the investment climate for U.S. companies overseas is not unnecessarily compromised.

To start that process, today the subcommittee has a panel of witnesses with unique abilities to discuss the operations of and challenges that CFIUS faces. This hearing and their testimony is intended to prepare members to make wise and cautious decisions on this vital topic. This should provide the beginning of a strong and thoughtful review.

With that, I would now recognize a member of the Democratic side, the gentleman from Washington, Mr. Heck, for 5 minutes for an opening statement.

Mr. HECK. Thank you very much, Mr. Chairman. And, Mr. Chairman, to begin with, I would ask unanimous consent to enter into the record a letter I sent to you and the Chairman of the full committee on December 8 requesting that a witness from the Department of Treasury be added to this hearing.

Chairman BARR. Without objection.

Mr. HECK. Thank you.

While I look forward to hearing from today's witnesses, I believe, frankly, there is no substitute for hearing from people who actually are administering CFIUS. I have given Treasury a very hard time in this committee—some of you may recall it was a very hard time—about this issue in past hearings. I want to make clear that they have begun to engage in what I would characterize as a constructive manner. I acknowledge that and express my hope that the committee could benefit from their expertise during a future hearing. I would be happy to yield to Chairman Barr if he would like to respond.

Chairman BARR. Yes. I appreciate the gentleman yielding. And just to clarify, this is the first of a series of hearings. We most certainly will be extending an invitation to Treasury officials who obviously have a large role in the CFIUS process to testify, and you will have that opportunity. I yield back.

Mr. HECK. Again, thank you very much, Mr. Chairman. I am glad to hear that, and I thank you, again, for convening this hearing.

I believe the CFIUS process generally works well for private, commercially motivated transactions. But in the 10 years since Congress last passed legislation dealing with this issue, we have seen some countries gain the resources and sophistication needed to pursue a comprehensive strategy to acquire U.S. technology, or dominate strategically important industries. Existing CFIUS authorities were not designed and are not sufficient to deal with that kind of challenge. And although, as many of our witnesses will note, this is a problem that every part of the U.S. Government will have to work together to address. I believe there are some aspects of this problem that can only be addressed through legislative action to close gaps in existing CFIUS authority.

When I asked Secretary Mnuchin about this in July, he agreed that this was a pressing issue, and that we could not afford to do nothing. I hope we can all bring that sense of urgency to how this committee approaches its work on CFIUS reform, the kind of ur-

gency and unity which I know this Congress can still bring to bear on issues critical to our national security, because here we are dealing with just such an issue.

And there are certainly things we need to keep in mind as we move forward. I am glad many of today's witnesses have raised issues, will raise issues like the need to improve information sharing and cooperation with our allies and partners, many of whom are also in the process of reevaluating their own CFIUS equivalents. I am glad many of today's witnesses will raise the need to provide more resources to CFIUS, which I agree are urgently needed to keep pace with the times, and the demand, and the need. And I am proud that the United States is, in fact, a place that welcomes foreign investment.

But the broader legitimacy and acceptance of that principle of openness, which I believe in, and the ability of the United States to stand up for a free and open global economy, is, in fact, dependent on our national security. As Secretary Mnuchin affirmed, doing nothing is not an option. But I am confident that starting with this hearing, we can find a bipartisan path forward, and strike that balance between continuing to allow robust foreign investment, which I think does serve our Nation's needs, our economic prospects, while at the same time, balancing it against very legitimate security concerns, which are growing in number, in velocity, and in complexity.

CFIUS needs to be reformed. It starts here with this committee, and it starts here with this hearing today, Mr. Chairman. So, finally, thank you, again, very much, for convening it.

Chairman BARR. Thank you. The gentleman yields back.

And today we welcome the testimony of the Honorable Mr. Kimmitt, a Senior International Counsel at WilmerHale. From 2005 to 2009, he served as Deputy Secretary of the U.S. Treasury, where he had significant responsibility for the Department's international agenda, which included a revamp of CFIUS. He also served in the Reagan White House as National Security Council Executive Secretary and General Counsel from 1983 to 1985. During 1997, Mr. Kimmitt was a member of the National Defense Panel, and from 1998 to 2005, he was a member of the Director of Central Intelligence National Security Advisory Panel.

Mr. Kimmitt served in combat in Vietnam with the 173rd Airborne Brigade, retired as a major general in the Army Reserve, and also served as the U.S. Ambassador to Germany.

The Honorable Mr. Estevez is a national security strategy and logistics executive at Deloitte Consulting, who served for 36 years at the Department of Defense. From 2013 to January 2017, Mr. Estevez served as the Principal Deputy Under Secretary of Defense Acquisition Technology and Logistics. In this position, he represented the Department of Defense at CFIUS while Chinese investment in the United States accelerated rapidly. Previously, he held several key positions, including Assistant Secretary of Defense for Logistics and Materiel Readiness and Assistant Deputy Under Secretary of Defense for supply chain integration.

The Honorable Mr. Wolf is a partner at Akin Gump, and from 2010 to January 2017, he was the Assistant Secretary of Commerce for Export Administration. In this role, he was primarily respon-

sible for the policy and administration of the U.S. dual-use Export Control System. And as a result of the export control reform effort, he helped lead part of the defense trade system. Also during this time, Mr. Wolf was the primary Commerce Department representative to CFIUS.

Mr. Segal is the Ira A. Lipman Chair in Emerging Technologies and National Security and Director of the Digital and Cyberspace Policy Program at the Council on Foreign Relations, an expert on security issues, technology development, and Chinese domestic and foreign policy. Before coming to CFR, Segal was an arms control analyst for the China Project at the Union of Concerned Scientists. He has been a visiting scholar at the Hoover Institution at Stanford University, the Massachusetts Institute of Technologies Center for International Studies, the Shanghai Academy of Social Sciences, and Tsinghua University in Beijing.

Ms. McLernon is President and CEO of the Organization for International Investment, an association representing the unique interests of U.S. subsidiaries of global companies. With a strong background in economics, her efforts focus on the important role U.S. subsidiaries play in the American economy and policy issues that would make the U.S. a more competitive location for foreign direct investment and job creation.

Prior to being named President and CEO, Ms. McLernon was OFII's Senior Vice President, where she focused on strategic communications and advocacy. Each of you will be recognized for 5 minutes to give an oral presentation of your testimony. And, without objection, each of your written statements will be made part of the record.

The Honorable Mr. Kimmitt, you are now recognized for 5 minutes.

STATEMENT OF HON. ROBERT M. KIMMITT

Mr. KIMMITT. Thank you, Mr. Chairman, members of the subcommittee. Thank you for your invitation to offer perspective on the Committee on Foreign Investment in the U.S. This is one of those rare instances where advancing age, including three decades of service on CFIUS, has some benefits.

My experience with CFIUS began in 1985 as Treasury General Counsel under President Reagan and Secretary Baker. As you noted, Mr. Chairman, CFIUS was then governed by an Executive Order signed in 1975 by President Ford because of concern about Saudi petrol dollars being recycled to buy American assets.

By 1988, concern had shifted to Japanese purchases, which lead to passage of the Exon-Florio amendment. And in 1992, concern about state-owned companies buying sensitive U.S. technologies lead to passage of the Byrd amendment.

In 2005, I returned to Treasury as Deputy Secretary. After deals involving the Chinese National Overseas Oil Company and Dubai Ports were blocked by Congressional concerns, Congress passed the Foreign Investment and National Security Act of 2007.

Today, growing concern about Chinese investment, particularly by state-owned enterprises, and especially in the technology sector, has led to legislation proposed by Congressman Pittenger, Senator

Cornyn, and bipartisan cosponsors. I would like to offer some observations that may assist in your deliberations.

Earlier this year, this committee helped legislate the Secretary of the Treasury as a statutory member of the National Security Council, demonstrating that U.S. economic strength is tightly linked to our overall security. And foreign direct investment (FDI), as both you and Mr. Heck have noted, Mr. Chairman, makes an important contribution to the U.S. economy. Almost 7 million Americans will receive their paychecks this month from companies headquartered overseas. Close to 40 percent of those workers are in manufacturing jobs. And, as you noted, FDI jobs pay about 25 percent more than the economy-wide average.

A more open investment policy is integral to U.S. economic success, and I urge President Trump to issue the traditional U.S. open investment policy statement at the earliest opportunity. But in issuing that statement, it is important to make clear that the U.S. Government must ensure foreign investment does not harm U.S. national security interests.

Chinese investment has an appropriately high priority for close scrutiny, because China seeks to compete strategically against the United States in multiple spheres: Military, diplomatic, and economic, using all elements of the state, including state-owned enterprises in that competition. Current legislation provides significant authority to block troublesome Chinese acquisitions. As you noted, Mr. Chairman, the first acquisition unwound by a President was under George H.W. Bush in 1990. Huawei's acquisition of 3Com did not proceed under President George W. Bush, and President Trump recently blocked the acquisition of Lattice Semiconductor by a Chinese investment group.

As you consider new legislation, then, I would be sure to address actual gaps in existing authority. There is particular concern the Chinese companies may be using creative legal structures to conclude deals short of ownership and control that could nonetheless impair U.S. national security. I believe this is a very valid area of stricter scrutiny in the United States. I would be careful, however, about extending CFIUS' reach to transactions occurring outside the United States.

CFIUS is intended to give the President exceptional authority to protect the United States without, however, superseding important authorities in other statutes. For example, if a joint venture abroad raises concerns about technology transfer or compromise, the export administration regulations, or international traffic in arms regulations, should be the first line of defense.

Although additional legislative authority is warranted, the greatest problem facing CFIUS today is a lack of resources. As cases filed before CFIUS climbed to 250 this year, and with the prospect that CFIUS agencies lead by Treasury could be involved next year in a major legislative and regulatory implementation exercise, the increase in workload may begin to delay jobs-producing investments that do not raise national security concerns.

I urge that matching requirements to resources continue to be a central point in your further deliberations. Today's hearing, and your future actions, are also being watched closely overseas. Of particular concern, the European Commission (EC) in Brussels is

establishing an investment review mechanism even though, under European law, the Commission has no authority or jurisdiction on national security matters. So the new EC review may become a political screening process that could create a new barrier to U.S. investment into that important market of over 300 million consumers.

In conclusion, I am more concerned today about growing investment protectionism than trade protectionism. If we want to grow well-paying jobs in the United States through foreign direct investment, we must send a clear message that the United States is open to investment except in those instances where a CFIUS process focused squarely on national security determines an investment must be blocked. I know you will strive to strike that important balance. Thank you.

[The prepared statement of Mr. Kimmitt can be found on page 38 of the Appendix]

Chairman BARR. Thank you. The gentleman's time has expired.

STATEMENT OF HON. ALAN F. ESTEVEZ

The Honorable Mr. Estevez, you are now recognized for 5 minutes.

Mr. ESTEVEZ. Chairman Barr, distinguished members of the committee, thank you for the opportunity to appear before you today and discuss the Committee on Foreign Investment in the United States, or CFIUS. While I am now at Deloitte, I do want to be clear that my views today are my own views, not those of my firm.

I believe it is important to review while CFIUS is critical to the national security from the DoD perspective. There are many reasons that the United States has the finest military in the world, most importantly, the men and women who volunteer to join that force. However, another reason is the technological superiority of our military force that we have over our adversaries. CFIUS is one of the tools that helps our military retain its technological advantage. Based on my experience, the CFIUS interagency process not only worked, it worked well in protecting national security of the United States for those cases that CFIUS had jurisdiction over. I never signed off, nor did I ever ask the Deputy Secretary of Defense to sign off, on a CFIUS case resolution that, in any way, would imperil national security. The DoD always achieved the mitigation terms that we asked for or received committee support to propose a block for those cases in which mitigation was too risky.

When I assessed the national security risk involved in each CFIUS transaction, I used the construct which I called the three C's, plus one. The C's represent the country, company, and commodity, commodity including technology. The plus one was co-location. That is when a foreign company was buying a company that was located near a sensitive military installation.

The framework worked like this: For country, we assessed if the home country of the purchasing party was a potential adversary of the United States, or if the country was lax in its protection of technology or personally identifiable information.

In assessing companies, we would determine if the company was a state-owned enterprise, or whether the company had been cre-

ated for that specific deal, or if the company or its ownership was reliable and stable.

To assess commodities or technology, we would review the criticality of those technologies to DoD weapons systems, both current and future, how cutting edge the technology was, and whether the technology was already globally available.

In co-location cases, we would assess what activities were taking place at a given location and whether the purchasing party would be able to observe or impact those activities.

If we had concerns with two or more of those C's, my experience was that such cases were heading to mitigation, at a minimum, or potentially a block.

I would like to now turn to areas where I believe CFIUS needs expanded authorities. I recognize that there are proposals currently being reviewed by Congress. My comments aren't based on that specific piece of legislation. The first area is joint ventures. While the vast majority of joint ventures do not threaten national security, some joint ventures may put national security at risk through technology or intellectual property transfer. Bankruptcy is another area where I believe we need to expand CFIUS authorities. Bankruptcies of U.S. companies, especially those involved in cutting-edge technologies, could end in the sale of technology or intellectual property assets to countries or companies of concern.

The final area I believe we need to assess with regard to CFIUS authorities is what I call connecting the dots. During my time as the DoD CFIUS representative, we noticed trends in which specific countries and companies were engaged in multiple transactions involving industry segments.

Most times, the companies and technologies being purchased were relatively small. They were not State-of-the-art, and they were not critical to national security. Nonetheless, I believe there comes a point where too much of a particular industry segment is under foreign control and this may put national security at risk.

The last area I would like to address is resources. The reality is just to process, manage, and mitigate the cases in the current workload, CFIUS needs more resources. The cases coming before the committee are growing in their complexity. Resources are needed to adequately perform the due diligence on the cases, to radically assess unfiled transactions, and to radically perform mitigation and oversight.

I thank the committee for holding this hearing. This is a critical topic for continuing long-term viability of our technical superiority. I look forward to your questions.

[The prepared statement of Mr. Estevez can be found on page 34 of the Appendix]

Chairman BARR. Thank you. The gentleman yields back.

The Honorable Mr. Wolf, you are now recognized for 5 minutes.

STATEMENT OF HON. KEVIN J. WOLF

Mr. WOLF. Thank you, Chairman, other members, for inviting me and holding this hearing on a very important topic. Although I am now a partner at Akin Gump, also my views are my own. I am not speaking for or against any particular legislation. Rather, I am here to answer your questions about how the CFIUS and the Ex-

port Control System worked. I am also not going to speak about any case that Alan or I or others worked on or that is before CFIUS now.

The other panelists have already described very well how CFIUS works, and we will get into that. So I want to get straight to my main point, which is that CFIUS and the Export Control System complement one another. CFIUS has the authority to control, and regulate, and block the transfer of national—technology of national security concerns if there is a transaction however defined. The Export Control System, the very purpose of the Export Control System, is to regulate the transfer of technology, regardless of whether there is an underlying transaction. This means that if specific concerns arise with respect to any particular type of technology, whether it is part of a CFIUS review or any other activity of U.S. Government, that the Export Control System, the rules governing the flow of goods, technology, software, and services out of the United States, should and could control that technology of concern to specific destinations, specific end users, and specific end uses.

Now, I realize that identifying, describing that technology, particularly dual U.S. technology that has both benign commercial applications, as well as military and other applications, is complex. I also realize that the Export Control System itself is very complex.

However, the system is designed, it was created, to constantly evolve to address new threats, new technologies, new issues, new end users of concern. In particular, the export administration regulations at the Bureau of Industry and Security, where I was for the previous 8 years, has the authority to impose these controls and alter them in coordination with, largely, the Departments of Defense, State, and Commerce. The descriptions of technology can be as broad or narrow as the concern arises. The scope of the controls can apply to specific entities, or entire countries, or they can apply to particular end users and end uses.

Most of the export administration regulations implement multilateral controls that are controls that are agreed to by between 30 and 40 other allied countries with similar concerns. And this is a reflection of the fact that multi-lateral controls, controls that our allies all work on together, are the most effective because they achieve a common objective.

It is also a reflection of the understanding that unilateral controls, controls that are imposed only by one country, generally tend to be counterproductive, because they result only in harming the industry of a country imposing the controls and don't actually block, in the end, the technology to the country of concern.

So recognizing these two competing structures, and recognizing that the multi-lateral system can move very slowly because it is a need for consensus with our allies to decide which technologies to impose, we created, during my time, a unilateral process to be able to tag and identify sensitive technologies of control unilaterally in order to be able to address the threat quickly and tailor it to whatever the concern is on the condition that eventually, it gets presented to the multilateral regimes for controls there.

There are many additional tools in the export administration regulations that can be tailored, such as a process of informing particular companies about particular technologies and particular end

users, again, regardless of whether there is an underlying transaction that there is technology of particular concern.

I focused in my comments here in the first 4 minutes on just technology transfer issues. But with respect to CFIUS, you also need to keep in mind that the national security issues we looked at are co-location issues, transactions involving those that create espionage or cybersecurity vulnerabilities, those that could reduce the benefit of U.S. Government investments, transactions that would reveal personally identifying information, those that would create security of supply issues for the Defense Department and other Government agencies, those that would implicate law enforcement issues, and those that would create exposure for their critical infrastructure such as telecommunications. Each one of these individual topics has their own issues and warrants their own hearing. So I am here because I have a 3-minute, and a 30-minute, and a 3-hour, and a 3-day version. I will stop here with the 5-minute version and be available for your questions over the course of the hearing. Thank you for inviting us.

[The prepared statement of Mr. Wolf can be found on page 55 of the Appendix]

Chairman BARR. Thank you, Mr. Wolf.

Mr. Segal, you are now recognized for 5 minutes.

STATEMENT OF ADAM SEGAL

Mr. SEGAL. Chairman Barr, Ranking Member, members of the committee, thank you for inviting me here today. My purpose is to provide a context for Chinese activities and what the motivations and challenges might be. I am going to make three points. The first is that China has a comprehensive strategy to move up the value chain and develop high technologies for national security and economic interests. That strategy involves many parts. It involves increased investments in R&D and in science and technology, industrial policy, and, in particular, policies focused on semiconductors, artificial intelligence, and what is called Made in China 2025, which is the use of the Internet of things and automation in manufacturing. It has its own foreign investment regime, which forces foreign companies to transfer technology, and fails to protect IPR, and is involved in cyber and industrial espionage, and then, finally, is involved in foreign acquisitions.

So can it acquire those technologies in the United States, Europe, India, Israel, and other locations? The policy that China has adopted is broad and comprehensive, and any U.S. response will similarly have to be broad and comprehensive.

Second, as a number of people have already noted, the investment decisions behind Chinese firms is often opaque. Who the actors are is opaque. They may say that they are private. They may, in fact, be private, but still receive significant support from state-owned enterprises. They may have tight connections to local or provincial governments. And so, the sources of the money and the motivations of that money are often unclear. They may be strategic. They may be economic. They may be hiding money from a corruption scandal.

The problem is compounded by the fact that President Xi Jinping has accelerated a process that was started under President Hu

Jintao of civil military fusion. And that goal is to tightly link the civilian and military economies so that any benefits that are brought to the civilian economy are eventually turned into military strength as well. And so that means that in this context, any advantage that is brought to the civilian economy could also be brought to the military economy.

Third and final, while I support many of the specific reforms that have been mentioned about increased capacity, increased information sharing, and other points for CFIUS, it is extremely important to point out that the U.S. and Chinese technology platforms and systems are increasingly integrated. We have seen that in information technologies where it is very, very hard to draw a line between where China starts and where the United States starts. We see a massive flow of people back and forth. We see co-investment.

We see a huge amount of co-research and co-writing of research papers. When Chinese scientists look for co-authors, they look to the United States. Over 40 percent are U.S. authors. And this pattern is going to be reproduced in these new areas of frontier technology.

So we already see this in AI, in artificial intelligence, that the two systems, although right now are often cast as competitors, as running a race against each other, they are going to be tightly integrated. And Google's announcement yesterday that it was setting up an R&D center inside China is just the most recent example of how tightly linked those systems are going to be. That means that for any type of either export control law or CFIUS reform, there is a high degree of chance that we could, in fact, hurt ourselves, that we would be affecting science and technology that feeds back into the U.S. system that drives U.S. companies and drives U.S. innovation.

Thank you very much, and I look forward to your questions.

[The prepared statement of Mr. Segal can be found on page 47 of the Appendix]

Chairman BARR. The gentleman yields back.

Ms. McLernon, you are now recognized for 5 minutes.

STATEMENT OF NANCY MCLERNON

Ms. MCLERNON. Chairman Barr, Ranking Member Moore, and other distinguished members of the subcommittee, thank you for your invitation to testify this morning. I am Nancy McLernon, and I have the pleasure of being the President and CEO of the Organization for International Investment, OFII, the only business association exclusively comprised of U.S. subsidiaries of international companies. Our members represent a wide variety of industries from companies headquartered all over the world, including Siemens, Lego, Samsung, and BAE. I applaud this subcommittee's effort to take the time to examine the economic importance of foreign direct investment to America's economy, and the effectiveness of the CFIUS process.

OFII's mission is to ensure the United States remains the most attractive destination for foreign direct investment due to the outsized impact it has on the economy and work force. 6.8 million workers in the United States take home a paycheck from an international company, including 20 percent of the U.S. manufacturing

work force offering 24 percent higher compensation than the economy-wide average. And somewhat counterintuitively, international companies manufacture in the U.S. not just for our consumption, but also for worldwide consumption. In fact, U.S. workers at international companies produce about 25 percent of all U.S. exports.

International companies are also tied to their communities. They provide world-class training and—world-class work force training and help strengthen the communities in which they sustainably operate. For example, Toyota, whose Kentucky plant is the largest manufacturing facility in the world, is applying its manufacturing know-how to help children's hospital reduce infection rates with a neonatal intensive care unit, decreasing infection rates by 80 percent. Think about it, a Japanese company, in Kentucky, the largest manufacturing facility they have in the world.

Historically, the vast majority of FDI flows into the United States through mergers and acquisitions in line with other advanced economies. And the vast majority of that cross-border investment flows into industries totally unrelated to national security. For example, Loreal's successes have been achieved by their strategic acquisitions here. They have expanded their footprint in the United States to include research, manufacturing, and distribution facilities across 13 States. In fact, I recently had the opportunity to go out to a facility in Little Rock, Arkansas that was the result of an acquisition of a Maybelline facility. Now that facility is the largest cosmetic manufacturing facility in the world in Little Rock, Arkansas, a French company manufacturing for consumers all around the world.

Indeed, examples like Loreal demonstrate that when global companies acquire or merge with U.S. companies, they often raise the industry's economic performance, become reliable commercial and investor anchors, making large capital investments, and reinvesting U.S. earnings into their operations here. Without cross-border M&A (mergers and acquisitions), our economy would not receive the full benefits that international companies provide. A critical factor in the attraction of the U.S. to foreign investors is our country's commitment to the rule of law, and the stability of the regulatory environment. FINSA (Foreign Investment and National Security Act), as was mentioned earlier, the result of extensive deliberations in Congress, laid the foundation for success. Importantly, during 2008, Congress engaged in an equally thoughtful process to implement FINSA. The resulting regulations carefully captured the balance that Congress sought, providing helpful guidance on the kind of transactions that are within the purview of CFIUS and the wide range of factors relevant to national security assessments.

Based on publicly available information and anecdotal experience of OFII members, it seems clear the CFIUS process is under stress. There appears to be more investigations and mitigation agreements, withdrawals of cases, and a lengthening period for resolution. Our members report that although CFIUS staff members continue to impress with their long hours and attention to unique circumstances, resource constraints are straining CFIUS' ability to handle its current workload. Such delays increase the risk to for-

eign-owned bidders in an M&A auction process, potentially forcing them to pay a premium.

But let me underscore that the international business community supports the efforts of CFIUS to ensure America remains safe, and we are in full agreement national security should be paramount. Yet, I caution that CFIUS should not be viewed as a panacea to address all the concerns that have been raised. The Government has a wide variety of tools at its disposal, ensuring fairness, predictability, and efficiency in national security reviews must remain the tenets of the CFIUS process. Any changes to the process need to be done thoughtfully with the full awareness of the economic states.

Once again, thank you, Mr. Chairman, I look forward to answering your questions.

[The prepared statement of Ms. McLernon can be found on page 43 of the Appendix]

Chairman BARR. Thank you.

The Chair now recognizes himself for 5 minutes for questioning. I appreciate the witnesses' outstanding testimony, very illuminating and educational.

Mr. Kimmitt, let me start with you because of your background in the development and evolution of CFIUS and your expertise. Obviously, as Ms. McLernon was pointing out, foreign direct investment is critical to the U.S. economy. She mentioned Toyota in Kentucky. But in my home State of Kentucky, foreign direct investment supports 117,000 jobs, a little more than 7 percent of the entire employment.

At the same time, as many of the witnesses pointed out here today, national security of our country is of critical importance. And FDI, if not carefully watched, could enable our enemies to inflict harm not just on our economy, but create a whole lot of national security concerns. And I will just quote the U.S.-China Economic and Security Review Commission, "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." The central question of this hearing is, how can we balance both the desire for strong foreign investment and strong national security? And can you give us a little bit of guidance on that?

Mr. KIMMITT. Mr. Chairman, I think you put your finger on it just precisely: Striking that balance that not only you as a subcommittee and committee seek to do, but really, what the members of the Administration do on a daily basis. I think it is important to reiterate that the U.S. is open to investment for the reasons that you and others have mentioned. At the same time, no one serving in public office has a higher responsibility than protecting the national security. I think we start out from the point of view that we are looking for ways to attract good, high-paying FDI jobs to the United States. Appearing before this committee now almost 30 years ago, my then boss, Jim Baker, said that foreign direct investment was our ace-in-the-hole. As Nancy said, it is foreign companies deciding that our marketplace, our system, and our workers

are worth that investment. I think that is where we start. But that is not where we end. We have to look precisely at those security considerations you mentioned.

And I think today, unlike past concerns—the Saudis, perhaps the Japanese—we are talking about someone who not only wants to be a peer competitor, but a peer winner against the United States. That is China. And we have to look at Chinese investment particularly closely. That doesn't exclude that there could be Chinese investment that does not raise national security concerns. It doesn't exclude that there could be Chinese investment that needs to be regulated or looked at by others. But I think, again, we start with the point of view that we want to attract that investment, but not at the cost of harming U.S. national security.

Chairman BARR. And, Ms. McLernon, what interests me about this issue is why there are not robust—sufficiently robust capital markets in the United States to provide alternative sources of capital for startups, or for mature companies in financial distress. Is there an alternative to foreign direct investment? And why do we not have strong enough capital markets in the United States to provide that capital as an alternative to a Chinese entity?

Ms. MCLERNON. Yes. Well, I would start with the fact that we don't want to close—we don't want to close our borders to foreign direct investment, right? So even if there was a way to try to figure out how to fund through our capital markets here, we don't have all the answers. And foreign companies, when they come to the United States, they don't just bring capital. They bring innovation. They bring world-class work force training, as I mentioned. They bring new ways to do things. We have seen that in the auto sector, right?

So I don't think that it would be a desire to wall us off and think that we have all the smarts, and we can have all the answers if we just contain it here. And the reason why we don't—we have had many people on the panel, and you yourself talked about the amazing benefits that foreign direct investment mean to the U.S. economy and to the workforce. So I wouldn't even think that would be a goal.

Chairman BARR. In the remaining time, Mr. Estevez, observers have said that the CFIUS process offers the view that other committee members somehow rolled the Pentagon on a decision or that the brass at the Pentagon somehow caved to outside influences and ignored input from Pentagon staff. Can you elaborate on that?

Mr. ESTEVEZ. I will. I don't think that is true. Inside the Pentagon—when I looked at a case, we brought in all the pertinent parties from the breadth of the Pentagon, there were military services, key agencies like National Security Agency, who have concerns on cyber cases, for example. And I always got the signoff at the senior leadership level. We always went into a case looking to say—I believe in foreign direct investment too. And we need to have that flow of capital, and we need the innovation that that brings. But I always wanted to make sure that we were protecting national security in doing that. And we brought the full gamut of the Pentagon resources when we examined a case. My three C's construct—China was always a case that we looked at regardless of the next step. And then when we went to the committee, I had

to make the case. I could never say that the committee rolled me against. I was pretty far in my discussions—

Chairman BARR. Thank you. Thank you.

Mr. ESTEVEZ. —as Mr. Wolf would tell you.

Chairman BARR. My time has expired. Well, more than expired. I appreciate members' indulgence.

And now I would like to recognize the gentleman from North Carolina, Mr. Pittenger. And I would just note not only is Mr. Pittenger the author of the Foreign Investment Risk Review Modernization Act, he is also the author of the legislation that made the Treasury Secretary a member of the National Security Council. And, with that, I yield to my friend from North Carolina, and applaud his leadership on this issue.

Mr. PITTENGER. Thank you, Chairman Barr. Thank you for your commitment and leadership. And thank each of you for being with us today and your expertise and background. I would say, too, I am from North Carolina. We have the largest hog processing plant in the world in my district owned by the Chinese, Smithfield, 5,000 jobs.

Right across the border from me is a big textile plant owned by the Chinese. So I have a real interest in Chinese investments, foreign investments of all kinds. I have a great appreciation for that. Having said that, I certainly read the statement by President Xi regarding his clear vision for China, his 5-year plan to acquire, aggressively acquire, technology companies. They have been pretty focused on that since 2014. I think they have acquired 43 semiconductor companies, 20 of which have been in the United States.

To that end, it brings us enormous concern. And I think those concerns are shared by many other leaders who support our interest in reform of CFIUS. I would read you a few of them.

Attorney General Jeff Sessions says, "CFIUS 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."

Secretary Mattis, "CFIUS is outdated. It needs to be updated to deal with today's situation."

Director Coats, "We should do a significant review of the current CFIUS situation to bring it up to speed."

Admiral Rogers, NSA Director, "We need to assess the CFIUS process and make sure it is optimized for the world of today and tomorrow.

Does anyone disagree with those perspectives?

Thank you for that.

With that in mind, I would like to just ask you, Mr. Wolf—and thank you for your service. Again, you served as Assistant Secretary of Commerce for Export Administration. At that time, you were involved in providing relief in the arms embargo that the U.S. and EU had imposed in 1999, following the Tiananmen massacre. These efforts in export controls reduce—enabled through President Obama's Export Control Reform Initiative lead to a massive Chinese military modernization effort. And, of course, today the U.S. military faces a far more capable PLA because, frankly, I believe, of these efforts.

Under the same tenure that you had, it took half a decade to punish the Chinese for the actions by ZTE in selling what we have

in technology to North Korea and Iran. I worked on this. Ultimately, they were fined $1 billion. But it took a long time to get that done.

And I would just like to know from you how credible you believe you can be as a witness on this CFIUS process given the lapse and what has occurred through the time of your tenure.

Mr. WOLF. Thank you for the question.

With respect to the ZTE case, that was 2 years of my life pursuing the matter. And I was the one that signed the denial order in pursuing it. So I think we were actually extraordinarily aggressive with respect to that matter, and the record speaks for itself.

With respect to the export control reform effort, with all due respect, we did exactly the opposite with respect to China. The whole point of the reform effort was to make it easier with respect to trade with our close allies, NATO in particular, so that we would have more resources in order to focus enforcement attention and to strengthen the embargo with respect to China.

Mr. PITTENGER. The net effect, though, was that it provided the Chinese access and greater capability as a result of what occurred and did not occur.

I would like to clarify for this committee what we intend not to do in the bill. The bill does not impose a ban, or automatically block all Chinese investments or that being of any other country. It does not require CFIUS to consider investment reciprocity as part of this bill. It does not cover all joint ventures. Joint ventures are a concern, but it does not cover all of them. It does not require any list of countries of special concern. No country is named in this bill.

It does not require any list of technologies or duplicate functions performed by the Export Control System. And it does not designate specific technologies that are to be safeguarded.

So I think there has been prudent consideration for what needs to be done and what should not be done. But I would convey to this committee and to each of you that without this type of clear focus and commitment, America's interests will be greatly threatened.

I yield back my time. My time is gone.

Chairman BARR. The gentleman's time has expired.

The Chair now recognizes the distinguished gentleman from Arkansas, an outstanding member of the committee, Mr. Hill.

Mr. HILL. I thank the Chairman. I appreciate our witnesses being with us today. Thanks for the effort to start this process, Mr. Barr, in evaluating how we adjust CFIUS' resource needs on behalf of the Administration, as well as balance the new challenges to our country. And I appreciate my friend from North Carolina taking a leadership role in the topic as well.

I would like to explore the issue, maybe starting with you, Ambassador Kimmitt, talking about the challenges of licensing technology as opposed to outright acquisition of it. Could you reflect on that and how that gets reviewed in the process?

Mr. KIMMITT. I would defer to my—

Mr. HILL. We will let others, too.

Mr. KIMMITT. —two panelists to the left. But what I would say is there is no definition of national security either in existing law or in the new bill. And I think that is very wise, because national

security is a dynamic concept. It is quite different today than it was during the cold war. To me, it is the summation of our foreign, defense, and international economic policies, all resting on a strong intelligence base. So when those CFIUS committee members come together, they have the responsibilities in their statutes, in their regulations, to protect national security at the fore. And particularly for State, defense, and commerce, licensing issues that are proceeding on another track are very often brought into CFIUS for consideration on the facts of that particular case.

I think it is really important to note that CFIUS shouldn't substitute for the work that is done on licensing, export controls, or other areas. But certainly, it needs to be part of that consideration. I just would make sure that CFIUS isn't leading in an area that I think is more properly the domain of State, Defense, and Commerce.

Mr. HILL. Somebody else want to comment? Mr. Wolf?

Mr. WOLF. Yes. Thank you. That is exactly my main point, which is if there is technology of concern, we should be controlled about the technology of concern and the transfer of it regardless of whether there is a transaction, regardless of whether there is a joint venture, regardless of whether there is an acquisition or a licensing arrangement. If we are going to spend the time, and attention, and government resources of identifying dual-use commercial technology of concern—and I grant everything that has been said today with respect to the underlying anxieties, and the motivations, and the concern, then we should do that.

And the Export Control System is specifically created, again, regardless of the nature of the transaction to control it, and without the collateral consequences of spooking or having an otherwise broader impact on foreign direct investment. And it can be tailored to the country, end user, and technology of concern without affecting the entire economic ecosystem.

So that is why I am an advocate for, to the extent humanly possible—it can't solve all problems. But if there is a technology concern issue, spend the time identifying that and working it through the system to regulate it accordingly.

Mr. HILL. And you think the statute gives you the ample authority to go through that process, identify that, and coordinate it inside the Executive Branch?

Mr. WOLF. The legislation is already there, absolutely, to already do that. It is a function of will, and resources, and time, and commitment. It is not a statutory issue.

Mr. HILL. And what about just—what is a bigger challenge of this country, foreign direct investment of sensitive assets, or just outright theft of American intellectual property?

Mr. WOLF. In my view, it is clearly the latter. That foreign direct investment, by and large, is not the issue, but the underlying tech transfer or IP theft that you are referring to can occur in many circumstances, not necessarily in connection with something captured by foreign direct investment.

Mr. ESTEVEZ. I would agree with that.

Mr. HILL. Something like 5 to 10 percent of exports are not exports. But export value is just sheer theft of intellectual property

from Europe and the United States. Would you agree with that estimate?

Mr. WOLF. I don't know the percentages, but that seems reasonable. I haven't looked at the exact data, but that seems reasonable, yes.

Mr. ESTEVEZ. That was always a concern of mine, things that weren't in our process, the CFIUS process. But cyber theft was a major concern. In fact, we put in some rules through—acquisition rules requiring companies to have at least a minimum standard of protection that were doing business with the Department of Defense to protect their IP that we were using.

Mr. HILL. Do you think inside the Executive Branch that that is—in today's world, since intellectual property, cyber risk, data security, true protection—I am not talking about just the trademark on Mickey Mouse, but I am talking about all of the above. Is that really adequately coordinated in the Executive Branch process? And is that—what is your view, having worked in it recently, as opposed to Mr. Kimmitt—we were centuries ago. We didn't even have email then. So talk to me, are we adequately coordinated there?

Mr. WOLF. No. I agree with the essence of your question, which is a lot more time and resources and commitment could and should be made to the effort of identifying those technologies that are commercial, that want control. Absolutely. Both—

Mr. HILL. Thank you.

Mr. WOLF. —and from an export control—

Mr. HILL. Thanks, Mr. Wolf. My time has expired.

Thank you, Chairman.

Chairman BARR. The gentleman's time has expired.

The Chair now recognizes the gentleman from Ohio, Mr. Davidson.

Mr. DAVIDSON. Thank you, Chairman. Thank you to our witnesses. I really appreciate your expertise in this vital matter for our national interests. And I certainly appreciate the importance of foreign direct investment in the United States. And we want to be clear that we are talking about things that would be counter to our national security interests, not things that would be counter to our national interests. We want foreign direct investment. We don't want to give away our national secrets, even at a high price, if they would jeopardize the security of our country.

I became concerned about this when I was a cadet at West Point. And in 1993, one of the first things the Clinton Administration did was transfer release authority for sensitive technology from Department of Defense to Department of Commerce. And we proceeded to sell, via Hughes, the capability to China to launch multiple satellites, in this case, not warheads, off of one launch vehicle. That seemed tantamount to treason to me at the time. But it was really a commercial decision. But it seemed really a bad thing for U.S. national security.

So I am really grateful to Mr. Pittenger and to the folks in this committee that have tried to address a modernizing of legislation that is post 1993 but really past due for some reforms. One of my big concerns is, where are the gaps, even with this legislation? What is left to be done? And so Mr. Hill talked about licensing. But

also, one of the big things that you see is startup companies, and venture capital, venture investing. And we spent a little bit of time talking about China. We are certainly not only concerned about the relationship with China. On balance, we benefit greatly from that trade relationship, with some real concerns about trade policy.

Here we are talking about national security. So putting aside countries, the kinds of mechanisms which were technology that we may still need to address beyond this CFIUS as it stands today.

Ms. McLernon, would you care to start?

Ms. MCLERNON. I think that you raise a number of very important issues. And there are a variety of different security experts on the panel other than myself.

I do think that it is important that we don't lull ourselves into a false sense of security. If we do focus only on one country and we ring-fence it, we risk being vulnerable to other areas of threat, and we also risk discouraging investment from that particular country that could actually benefit the U.S. economy.

Mr. DAVIDSON. Yes. Thank you for the clarification.

Mr. Kimmitt?

Mr. KIMMITT. I would say that your point about instances beyond normal M&A activity is really an important one, Congressman.

And let's remember that the current law applies not only in the cases of ownership but also control. And CFIUS looks very closely at investments, including in startups, where a foreign company or investor would have enough equity ownership and enough governance rights—board seats, observer status, accumulation rights, special voting rights—that that could trigger the CFIUS covered transaction rule.

I think, having spent 2 years, myself, running a software company in Silicon Valley, that isn't well-understood there. I think we need to do a better job of letting people in our technology hubs—not just Silicon Valley but the Research Triangle, down around Austin, around the country—know that they have to be careful as they take that foreign investment that it does not rise to the level of control, which would then trigger CFIUS.

And so, for example, if they are going to set up an investment fund, let's make sure any foreign limited partners are truly limited, that they are passive investors. I think that is an area that CFIUS actually looks at fairly closely, but I think, on the company side, particularly in that startup community, there is not as clear an understanding as there should be of what foreign investors, particularly any with malign purposes, may be trying to do.

Mr. DAVIDSON. Thank you.

Mr. Estevez?

Mr. ESTEVEZ. Well, first of all, I agree with Ambassador Kimmitt on that point.

We also have to watch the negative implications. So if you are a startup in Silicon Valley with some really cool technologies, I want those companies to do business with the Department of Defense. And I don't want them to not want to do business with the Department of Defense because suddenly we are going to put a fence around them. So—

Mr. DAVIDSON. Yes, correct. And I think the big thing is, and to your point—because my time has expired—the point is that a lot

of these early stage folks don't even realize the national security implications. It is a brilliant technology. It has dynamic, profound potential applications for our economy, for the global economy, but it could be used for nefarious purposes.

My time has expired. Mr. Chairman, I yield back.

Chairman BARR. The gentleman yields.

The Chair now recognizes the gentleman from California, Mr. Sherman, for 5 minutes.

Mr. SHERMAN. With Dubai Ports, we had a company that happened to be owned by the government, and that government was, at the time, supporting international terrorism.

Should we have in any CFIUS law a provision that says you explicitly must take into account whether the host government of whatever company is making the investment supports terrorism—whether or not is a state sponsor of terror?

Does anyone have a comment?

Anybody here think that we shouldn't take into consideration whether the company making an investment in U.S. assets is based in a country that supports terrorism?

Mr. KIMMITT. Mr. Chairman, I think at Treasury, which I know—

Mr. SHERMAN. Right.

Mr. KIMMITT. —a bit better, although the CFIUS process is run by the International Affairs Division, as you know, the people in TFI, Terrorist Finance, comment on every—

Mr. SHERMAN. They comment, but there is not an explicit provision that says: It might be a wonderful company buying a wonderful asset; it just happens to be based in Tehran. And there is nothing in the law that I read or that you can point to that says that that would be one of the factors, correct?

Mr. KIMMITT. There is nothing specifically in FINSA, although, as you know, in the wake of CNOOC and Dubai Ports, there was much greater scrutiny put on acquisitions by state-owned or—controlled entities.

Mr. SHERMAN. But I am not just talking about state-owned or—controlled entities.

Mr. KIMMITT. No, but I would say where you will find that specific language is in legislation that you have passed and Executive Orders that have been issued by the President on state sponsors of terrorism, including the Iranians and others. So—

Mr. SHERMAN. The government or private enterprises based in Tehran?

Mr. KIMMITT. I would say both—

Mr. SHERMAN. You would say it would be rejected just on that basis? Or what weight would it be given?

Mr. KIMMITT. Certainly, if it were a company based in Tehran, it would be rejected, I think, outright.

But I think the key point you are making—

Mr. SHERMAN. And maybe Dubai, we would look at it more carefully.

I would point out that we may be looking too narrowly when we look at ownership or control of a company, as if you have to have seats on the board to control them.

And I will give you one example. We have allowed a terrible situation in our weak position with China, so they are able to turn to Boeing and say, "We won't buy your planes unless you make the fuselages here in China." So they don't have anybody on the board, they don't own any stock, but they control corporate decisions.

Now, I don't know whether it was a fuselage or the wing assembly, and I don't know whether that poses a risk to our national security or intellectual property. But I do know that, once we consent to a situation where a country can have a huge trade surplus with us, over $300 billion, and then turn to our companies and say, "And you can't even sell your products here unless you transfer this technology, unless you build this plant here, unless the patents are located here, unless the computer system or cloud is located here," that we may be looking over at corporate ownership and not looking at corporate control. The fact is, if you can close your markets, you can control corporate decisions.

Another thing I will point out is that I think it is important to note that, if bad decisions are made by CFIUS, they can be reversed under the International Emergency Economic Powers Act. Now, that would be extraordinary; it has never been done before. But I think that, as we plan to revisit CFIUS, we should be aware of that act which could be used—and I cite 50 U.S.C. 1702—to reverse a bad decision.

And I yield back.

Chairman BARR. The gentleman yields back.

The Chair recognizes the gentleman from Minnesota, Mr. Emmer.

Mr. EMMER. Thank you, Mr. Chair.

And thanks to the witnesses for being here today.

So I want to go back to Chairman Barr's opening when he was talking about how does CFIUS balance national security versus foreign direct investment. And I want to tie it together with—I think it was something that Ambassador Kimmitt said about there is no definition of national security in the law.

So what is the priority for CFIUS when you are reviewing a transaction? Is it national security or is it foreign direct investment? Which one comes first and then has to be balanced against the other one? And when you are talking national security, I will just add, how do you define it?

And we will start with the Ambassador.

Mr. KIMMITT. My point only was that national security is a dynamic, ever-changing concept. It meant one thing during the cold war, another in the post-cold war period, post-9/11, and post-financial crisis.

And I think the important thing is CFIUS, which exists only to screen investments for national security concerns, has at the table every department and agency that is responsible for safeguarding the national security interests of the United States. So the Defense Department might bring their concerns about military technology. The State Department might bring, or Treasury, some of the concerns, for example, that Mr. Sherman mentioned about terrorist activity. Commerce will bring concerns about export controls. DHS and DOJ bring a very different set of concerns.

So, basically, each of the agencies is looking at the investment in an open investment policy environment. But the reason that they are there is to say, even though we are open to investment, are there any elements of this transaction, if concluded, that would raise concerns from our department or agency's perspective? If so, they need to be identified, addressed, mitigated. Or if they can't be mitigated, the deal needs to be blocked.

Mr. EMMER. Well, it doesn't look like—when I look at this summary, a total of 770 transactions over the last, what is it, 6 years, something like that, that are cited in this graph. There aren't many.

And I go back, and maybe Mr.—I shouldn't call you "mister"—the Honorable Mr. Estevez, you were talking about when you review something inside the Pentagon. There is a case that I tried to look up, because it is back from 2011 and 2012 involving Cirrus Airplanes in Duluth, Minnesota, that a Chinese company came in and put a purchase agreement together, and all kinds of red flags went up, because the argument was they are going to buy this very interesting technology, they are going to reverse-engineer it in China, so we lose the jobs, we lose the—it is great to want this foreign direct investment, but I think Mr. Sherman had a great point. You also have it going on with what Mr. Hill is talking about, with outright theft.

What happened—do you remember the case I am talking about? And is it one of the ones that was—there were 20 back in 2012 that the notices were withdrawn after commencement of the investigation.

Mr. ESTEVEZ. First, being a member of the committee, we don't really want to talk about specific cases, because the confidentiality of that process helps us dig into those companies. But the reality is I also don't recall that case, specific case.

Mr. EMMER. Well, no, and that is great, and I respect that. If I can just add, before I forget about it and let you finish, it would be very helpful if at some point down the road, when you think it is not hot anymore, where policymakers can actually see some of these cases and the deliberations that you go through. Maybe it would help us understand how CFIUS is working.

Mr. ESTEVEZ. On any case, we would have looked at the technology. And, again, it is not about—economic security is part of national security, absolutely. And we would discuss that, too, when we were discussing cases. But we would look at the technology and say, is this technology state-of-the-art? Is it useful militarily, that it would advance their capability, whoever "they" are, in this case China, over ours? And if there was any doubt about that, I would be in there arguing that we either have to put control around this, depending on who the company was and the country was and whether we would trust them on those controls, or I would be arguing for a block.

Again, as the Honorable Mr. Wolf sitting next to me would say, I was usually sitting there pounding the table saying this—

Mr. EMMER. Yes, but then you could get overruled.

Mr. ESTEVEZ. Never.

Mr. EMMER. OK. Good.

I see my time has expired. Thank you.

Chairman BARR. The gentleman yields back.

The Chair recognizes the gentleman from Illinois, Mr. Foster.

Mr. FOSTER. Thank you, Mr. Chairman and to our witnesses.

Let's see. Mr. Segal, in your testimony, you mentioned things like source code as one of the things that are hard to keep under control when you get an investment. And are there investment models that allow us to accept money but keep the intellectual property here, or is that pretty much a lost cause once you have a significant investment?

I am happy to have everyone—is there a workable model of that? Or once you have someone who has a 20-percent stake, they are going to want to see a review of the technology on regular intervals and want to have basically, people injected into the company and see both the present and the future intelligent developments? Any way to keep that from happening?

Mr. SEGAL. Thank you.

I think that that specific case refers to investment inside of China. So when—

Mr. FOSTER. OK. It was just an example of the sort of intellectual property that is hard to—that is hard to keep in one place.

Mr. SEGAL. So I think it would go back to Ambassador Kimmitt's point that when you are investing in a startup or another technology company, what percentage control you get, what the terms are, and what access to the information, I think those are often individually negotiated. And then it would have to be brought to the attention, depending upon what the source code was, what the technology was, that was to be transferred.

Mr. FOSTER. And is there a retrospective look at how successful those have been in keeping the technology from escaping? Or this is a one-time decision and then you don't look back 5 years later and see if the technology has actually not been adequate?

Mr. ESTEVEZ. So we would always look at the technology and see, again, how cutting-edge it was and how it would impact potential adversaries' capability, again, from the Department of Defense perspective.

And not only would we look at the technology itself, we would look at the industrial process. So some companies are better at doing things than other companies, and we wouldn't want the secret sauce, if you would, to migrate overseas if it was a very state-of-the-art company.

We would consider all those things. If we thought we could mitigate, we would propose the mitigation on how to wall off the fact that there was foreign cash going into the company. If we didn't think we could do that, we would propose a block.

Mr. FOSTER. And when you believe you have walled it off, do you then have a process in place to review how successful that walling off has been?

Mr. ESTEVEZ. If we propose mitigation, we would enforce that mitigation agreement in perpetuity. So you were assessing how that was working.

Now, with that said, I will go to my earlier testimony: There are not enough resources to continue doing that, especially as cases get more complex.

Mr. FOSTER. And if you look further into the future, it is easier to catch up than to develop new technology that doesn't previously exist. And so, in the medium/long term, we are going to be coequals with many countries in Europe and Asia in a lot of areas.

And so then the question is, do we have a structural disadvantage? Or will it become as easy for us to invest and get their technologies moving back in areas where they are ahead of us? Or is that something where we should start negotiating now to make sure we haven't built in a structural disadvantage as coequals? And this is in a world where we are coequal technologically.

Mr. SEGAL. Well, I think, in particular with the case of China, we do want to insist on greater reciprocity. There are a number of sectors in high technology that are still off limits for U.S. investment. The amount of openness and access to U.S. R&D, U.S. universities does not exist in the Chinese case. So, as China becomes a more capable player, I think it behooves us to insist on greater reciprocity and access to those resources.

Mr. FOSTER. Now, in addition to absolute cutting-edge technological spaces, a lot of the future military applications are going to be things like drone swarms, like just massive numbers of security cameras, things like that, where it is actually the price that is as important—the mass production of very large numbers of relatively low tech, where "low tech" includes cameras with facial ID and things like that.

And I was wondering, is there a lot of concern that, even though the technology might not be leading-edge, that just the very high-volume manufacturing is another area where we could fall behind and have to protect the technology?

Mr. ESTEVEZ. Yes. Let me address that very briefly.

We would look at the technology. If it wasn't cutting-edge, we believe that our innovation would pace that. And, more importantly, from a military perspective, our tactics, techniques, and the men and women that are in our forces constitute an advantage on how they use that technology that would pace whatever competitors there are in the globe.

Mr. FOSTER. All right. Thank you.

And I yield back.

Chairman BARR. Thank you.

The gentleman's time has expired.

The Chair recognizes the gentleman from Indiana, Mr. Hollingsworth.

Mr. HOLLINGSWORTH. Good morning. I appreciate all of the witnesses being here today. This is certainly an interesting topic and a vital topic that we discuss further.

Mr. Foster, my colleague, had brought up some of the ongoing monitoring, and I know Mr. Estevez had answered some of those questions. But I wanted to get back to that and talk a little bit about these monitoring agreements and how vital it is that we ensure what we set in place and the guardrails around that are continually being looked at and updated.

So I know you mentioned that resources are a problem. Can you talk a little bit about previous issues with resources, what resources might be required, what apparatus we have in place, what

apparatus we need in place, and just fill in some of the color around the ongoing monitoring agreements?

And others can certainly take the question as well.

Mr. KIMMITT. I would start at the general, let my colleagues go to the specifics.

I have spent a lot of time working in Government. Most of the energy and the resources go in on the upside—that is, until the policy decision is reached, the legislation is enacted—and we don't give the attention and resources to the implementing side of it, which is really important. You know that from your business time. You have to drive to results.

And so what I would say is let's make sure we have resources on both sides of that equation. And if in the middle of it is a mitigation agreement, let's make sure there is as much energy put into implementing and overseeing that mitigation agreement as there was in negotiating it.

That is where I think we run into a real resource problem. I think both in Treasury and in the interagency process more broadly we have barely enough people to address today's cases. And if you then have an increase in cases or implementation responsibilities because you pass new legislation, I think the place that is going to lose is on continuing to watch those mitigation agreements, make sure that they are faithfully executed, and, as Mr. Estevez said, very importantly, that we connect the dots across decisions that are made. That is where I think the resource constraint comes in.

Mr. ESTEVEZ. One other factor—and I fully agree with Ambassador Kimmitt on that—is that, as time elapses from the time a mitigation agreement is put in place—so if we did one for DoD in 2013, I remember it. I am gone. Some of the staff has turned over. Some of the outside directors that we put in have turned over. So I am real concerned about institutional memory that comes with resources to do that enforcement.

Mr. HOLLINGSWORTH. Yes. I think that both your comments are really, really thoughtful in ensuring that, ultimately, if we are going to make a certain decision, we need to have the resources to enforce those decisions.

And as you well said, if we are going to be faced with many more cases and resources are barely enough to even face those cases, if there is a probability any greater than zero that some of those will be accepted and there will be monitoring agreements, then resources need to be allocated to those monitoring agreements in the long term as well.

I wanted to specifically also ask of Mr. Wolf, was there ever a time in your tenure where you felt like you didn't have enough time to adequately review, thoroughly vet, and arrive at the right decision in your mind—

Mr. WOLF. No.

Mr. HOLLINGSWORTH. —that the process was rushed?

Mr. WOLF. No. I agree with Alan. We never cleared off on a transaction for which any of the departments believed there was an unsolved national security threat. To the extent we needed more time, there were withdrawals and refiling. And with massive ter-

rific support from the intelligence community, I am confident that, with all the cases we reviewed, we made it to the right outcome.

And to refer to a comment made earlier, they were never a balance—we were never balancing investment with national security. If there was an unresolved national security threat, we blocked or mitigated; we didn't balance. And so the answer to your question is no.

Mr. HOLLINGSWORTH. Well, that answer to the question certainly will help Hoosiers back home sleep better at night, knowing that we are thinking about those things and we are giving them the adequate amount of time to vet them.

And I really appreciate the comments. And I think this is something, more broadly, as you well said, as a problem, an epidemic across all aspects of Government, that we spend too few of our resources focused on the enforcement of a decision instead of just on the decision itself.

And, with that, I will yield back, Mr. Chairman.

Mr. KIMMITT. Mr. Chairman, could I just add one point, just picking up on the point that Mr. Wolf just made?

It is really important to understand the critical role that the intelligence community plays in the CFIUS process. When the case is filed, it is sent to the Director of National Intelligence for a community-wide look at the case. I would say, going to Mr. Foster's point, particularly some of the S&T considerations that need to be looked at very closely, and the DNI then comes back with a low, medium, or high assessment, that helps guide—it doesn't make the decision, but guide what the committee does. And then, as was mentioned, almost all of the major CFIUS agencies have their own intelligence elements inside. So there are almost two bites at that apple.

I think for looking ahead, that 5-year look-ahead, in addition to make sure that we implement correctly, we are really relying on the intelligence community to come with us not just on the instant concerns on these transactions but what are those trends, those 5- and 10-year trends that we need to be concerned about.

Chairman BARR. Thank you.

The gentleman's time has expired.

The Chair now recognizes the gentleman from Texas, Mr. Green.

Mr. GREEN. Thank you, Mr. Chairman.

I thank the witnesses for appearing today. I think this is an exceedingly important hearing. And I am very much concerned about assuring ourselves that we are on the right course.

Mr. Segal, you have indicated that unilateral action may not be sufficient, that there is something more that we have to do so as to protect our U.S.-originated science and technology. Would you give some additional intelligence on this, please?

Mr. SEGAL. The fundamental issue is that there are very few, if any, science and technology issues that the United States still monopolizes. And so, for any technology that the United States has decided that it represents a dual-use threat, it is very possible to go find, except for a very, very narrow range of technologies, similar producers.

To give just an example, on issues on cybersecurity or AI or computer science or technology, the Chinese are sending delegations to

Israel every week. And while the Israelis are more aware of our concerns about dual-use, they are not going to find in the same ways that we are in every instance.

So I think the issue is that, unless you have a fairly broad set of agreements among your partners, it will be very easy for Chinese actors to find most technologies in other markets.

Mr. GREEN. With reference to partners, are there certain institutions that can validate a partner's position such that we can feel more comfortable with it as opposed to someone that might not be associated or affiliated with the institution?

Mr. SEGAL. I may defer to Mr. Wolf, but I suspect that the intelligence agencies cooperate and share information.

Mr. GREEN. If you would, please.

Mr. WOLF. Sure.

To the extent that there is information about an entity that creates national security or foreign policy concern, my old bureau, Bureau of Industry and Security, had the authority to identify it publicly as an entity to which exports are blocked or other transactions are red flags.

And then, within the CFIUS review process, the intelligence community will provide to us information about other entities that might not necessarily be known to the parties, and we factor that into our decisions to either block or mitigate.

Mr. GREEN. What about NATO, a membership in NATO? Does that give you some degree of assurance?

Mr. WOLF. With respect to the country—as a country, absolutely. But it doesn't mean that every company inside each NATO country is, per se, not a concern. So we review not only the country of issue but the company, the personnel, the funders, people that may be behind it. So just because it is from Germany or France doesn't, per se, mean that there are absolutely no concerns.

Mr. GREEN. And how effective are we at spotting companies that have investors that may have ill intentions such that they are in a position to take advantage of knowledge that they acquire notwithstanding the fact that they look legitimate?

Mr. WOLF. Well, that is one—real quick, that is one reason for my emphasis on the focus on the technology. If the technology is of concern, it warrants review, period, regardless of who the parties are. And the licensing process gives the U.S. Government the opportunity to do a deep dive into who the investors or other parties are, as opposed to the other way around.

Mr. ESTEVEZ. And the intelligence community does a very good job of digging out all the facets of a company, including whether—who are the bad investors that may not be good actors.

Mr. GREEN. We have some sensitive areas in the United States where we have certain things being developed that are to be kept under wraps, for want of better terminology. Do we have any concerns about persons locating businesses in and around these very sensitive areas?

Mr. ESTEVEZ. If it was a covered transaction, we absolutely address that under the CFIUS regime.

Mr. GREEN. Well, my time is up. Thank you, Mr. Chairman. I yield back.

Chairman BARR. The gentleman's time has expired.

And with the witnesses' indulgence, we are about ready to have a vote on the House floor, but we will take the liberty of asking one final 5-minute round of questioning, with members' agreement here.

We heard from Ms. McLernon earlier that, although the U.S. capital markets are the deepest, most liquid and competitive in the world, in and of themselves, U.S. domestic capital markets are not sufficient to provide the level of financing that startups and other companies need, and foreign direct investment is a very critical part of financing of our companies in this country. And they provide, in the cases of foreign direct investment, many times, other assets other than just capital.

We also heard today that there are legitimate national security threats, and we need to strike the right balance.

So just in the remaining time, could each of you briefly—if you could identify one policy recommendation to improve the current or modernize the current CFIUS review process, what would that one policy recommendation be?

And we will start with Mr. Kimmitt and work our way down.

Mr. KIMMITT. I would go back to what has been the common theme, and that is we need to make sure that we have adequate resources both for the identification of potential issues, the review and adjudication of those, and then implementation of any agreement that might be reached, a mitigation agreement, to bring us to a "yes" answer.

And I would think it is very important, going back to Mr. Pittenger's point of the number of senior officials in the Administration who have talked about the need to reform CFIUS, I would just say I hope those senior officials will themselves get involved in the process both to identify the resources they need in their departments and agencies and empower their people involved in the CFIUS process to deal with these cases expeditiously on behalf of the American people.

Chairman BARR. Thank you.

Mr. Estevez?

Mr. ESTEVEZ. Of course, in my testimony, I address certain areas. There are many of the areas in Mr. Pittenger's bill. The resources need to be addressed.

But I would also say that CFIUS is one tool in the toolbox. We need to look at the gamut of our legal capabilities and what industrial policy and reciprocity that we might want to enforce across the board in our dealings with foreign nations and foreign companies. So, while CFIUS is one way to get at that, it is not just CFIUS.

And the final point I will make is you need carrots as well as sticks in this process.

Chairman BARR. Mr. Wolf?

Mr. WOLF. A significant, massive, whole-of-Government effort that is creative and digs into all the types of emerging technologies and other technologies that aren't on either of the control lists that are in commercial applications that are sensitive or of concern that have been discussed behind all the comments today. That requires a lot of agencies, a lot of creativity, a lot of attention, and a lot of resources, frankly, to do that.

With everything we are talking about today, it all depends, whether it is part of the legislation or export controls, on the ability of either CFIUS or the Export Control System to identify the technologies of concern, whether broadly or specifically. That is the work that is at the core of everything we are talking about today. And that is my policy recommendation.

Chairman BARR. Mr. Segal?

Mr. SEGAL. If the concern is primarily China, then I think we need to address all of the other forms of technology transfer that are occurring, so some of the issues of reciprocity that I mentioned before, as well as battling back on techno-nationalism in Chinese industrial policy.

On the CFIUS process itself, I echo the calls for resources and also, perhaps, new mechanisms for tapping into the expertise in academic and business communities about how the technologies are developing, which ones are going to be the ones we are worried about 2 to 5 years from now, and what types of joint ventures and other types of agreements our people are thinking about in the future.

Chairman BARR. Ms. McLernon?

Ms. MCLERNON. Let me just also echo the important need for resources. It is very hard to determine how well CFIUS works now and what the gaps are if they don't have the resources to do the job that is in front of them now. If we expand the scope, we risk leaving ourselves vulnerable and may take their eye off the true defense-related, national security concerns.

I don't think it was mentioned earlier the number of deals blocked. I don't think that that is an indicator of whether CFIUS is working. You have no idea how many deals don't even start because CFIUS exists. So I wouldn't look at those numbers, per se, that it wasn't functioning properly.

But I cannot emphasize enough the need for resources there, not only for national security but for our ability to be competitive. Because foreign-based companies are concerned now with the length of time that has to happen in order to get a review. So I can't emphasize that enough, as well as looking at other tools, that CFIUS cannot be the one and only thing that we focus on to protect our national security in this space.

Chairman BARR. Thank you.

And I would like to yield to the gentleman from North Carolina for a comment.

Mr. PITTENGER. Thank you, Mr. Chairman.

Thank each of you for being with us today. It is very, very meaningful to all of us.

I would like to enter into the record statements of support for CFIUS, which would include former Secretary of Commerce Penny Pritzker and Secretary Wilbur Ross, the Secretary of Commerce.

Chairman BARR. Without objection.

Mr. PITTENGER. I would also really like to thank Senator Cornyn for his leadership. It has been remarkable. He and his team have really worked very hard on this. It is been an honor to work with them.

I also would like to thank Secretary Mnuchin and Treasury. They have played a significant role in writing this legislation, along

with Chairman Nunes, who is a cosponsor of this bill, and Chairman Burr. Everyone has participated in a very significant way to make sure that we have a good perspective on what needs to be done going forward.

Thank you, Chairman Barr.

Chairman BARR. Thank you.

The gentleman yields back.

And for a final comment, I will yield to the gentleman from Illinois.

Mr. FOSTER. Well, I just want to thank you and, I guess, apologize for the attention deficit disorder of Congress on this sort of issue. And thank you, Chairman, for attempting to remedy that.

Because this is something where I think our Government and our Nation suffers from the lack of the long-term vision that you actually, frankly, see in China, that a lot of our investment model, where you are bonused on the quarterly profits as opposed to the 10-year performance of a company, causes us to not invest as strategically as we should.

And I hear you very clearly about the lack of resources. When we have some big mess like the Ebola crisis and so on, there is a big temporary spike in funding, and then it gets eaten away until the next time things become a crisis. This has been on ongoing crisis for more than a generation.

Now, one thing that occurred in some of your testimony was reference to intellectual property violations. And one of the reasons that we have to depend on foreign capital for things like venture capital is that, when you have a really good invention, like Microsoft Word, and then find that it gets pirated in other countries, you don't have the follow-on investment capital.

And I was just wondering if you see that as an important area where we have to—this would be a much smaller problem if there was a huge increase in the amount of venture capital available simply because we didn't have our inventions ripped off offshore.

There was a number, like, 150 billion of Chinese investment into startups? Was that a number that occurred in one of your testimonies? And that is probably small compared to the amount of software that gets stolen, for example, in China every few years. And so I think we have to keep our eyes on that one very strongly.

I just want to thank the Chairman for having this hearing. It is a big deal. And thank you.

Chairman BARR. Thank you.

I appreciate the gentleman, and he yields back.

And I would like to thank all of our witnesses for their testimony today. It was very educational, illuminated a lot of issues for the members.

As we indicated before, this subcommittee will continue to review the CFIUS process. We will have several more hearings at the beginning of 2018, and we invite the continued engagement of these witnesses and others as we continue to review and update this process.

And I would echo the comments that we do hear you loud and clear on the resources point, which was a unanimous point that was made here today.

Without objection, all members will have 5 legislative days within which to submit additional written questions for the witnesses to the Chair, which will be forwarded to the witnesses for their response. I ask our witnesses to please respond as promptly as you are able.

This hearing is now adjourned.

[Whereupon, at 10:43 a.m., the subcommittee was adjourned.]

A P P E N D I X

December 14, 2017

United States House of Representatives
Committee on Financial Services
Subcommittee on Monetary Policy and Trade

Examining the Operations of the Committee on Foreign Investment in the United States (CFIUS)

Opening Remarks of The Honorable Alan F. Estevez
Former Principal Deputy Under Secretary of Defense for Acquistion, Technology, & Logistics (2013-2017)

December 14, 2017

Chairman Barr, Ranking Member Moore, distinguished members of the subcommittee, thank you for opportunity to appear at this hearing and to testify regarding the Committee on Foreign Investment in the United States, or CFIUS.

While I am now at Deloitte, I want to be clear that the views I express today are my own. My expertise in this area derives from my previous position in government. I was the Principal Deputy Under Secretary of Defense for Acquisition, Technology, & Logistics, in an Acting capacity from 2011 to 2013, and confirmed in the position from 2103 to 2017. In that role, from 2011 to 2017, I managed the CFIUS process for the Department of Defense (DoD), and I was the DoD representative to the CFIUS.

Before I discuss my experience and views with regard to CFIUS, I believe it is important to review why CFIUS is critical to national security. There are many reasons that the United States has the finest military in the world, most importantly the innovative, dedicated men and women that volunteer to join the force. However, another reason is the technological superiority of our military force, or, in other words, our technological advantage over our adversaries. The US never wants to send our great force into a fair fight, we always want the advantage, and our technological superiority helps to ensure that. With that said, our technological advantage over potential adversaries has eroded. This happened for a number of reasons, to include the now 16-year focus on the war against terrorists, the inevitable globalization and commercialization of technology, and the devastating impacts of the Budget Control Act on DoD buying power. On the other hand, CFIUS is one of the tools that helps our military to retain its technological competitive advantage.

Based on my experience, the CFIUS interagency process worked, and, in fact, it worked well in protecting the national security of the United States. That does not mean that we did not have to adjust the process to make it more effective over time. However, I can say that over the hundreds of CFIUS cases that I processed as the DoD representative to CFIUS, I never signed off nor ever asked the Deputy Secretary of Defense to sign off on a CFIUS case resolution that would in any way imperil national security. In my view, the DoD always achieved the mitigation terms we asked for in cases that merited

mitigation, or received Committee support to propose a prohibition for those cases in which mitigation was too risky. This was true whether DoD was the lead agency along with the Department of Treasury, or the DoD was in support of another Department.

My second point is that current CFIUS authorities, along with the authorities in other Departments, such as the export control authorities of Commerce, allowed the Committee to properly adjudicate the wide variety of cases that came before the Committee. I'll address areas where I think authorities need to be expanded in a moment, but for the types of cases currently within CFIUS jurisdiction that we adjudicated during my time, we had adequate authorities to rely on.

When I assessed CFIUS transactions from the DoD perspective, I personally used a construct, which I called the three C's plus one. The C's represented Country, Company, and Commodity (which includes technology). The plus one was Co-location, that is when a foreign company proposed buying a company that was located near a sensitive military site. This framework helped me and my staff to assess the risk to national security involved in each transaction we processed. For each case, we would assess whether the home country of the purchasing party was a country of concern. The country of concern definition not only included potential adversaries or malicious actors, but also could include, for example, countries that were lax in protection of technology or were lax in the protection of personal identifiable information. This framework was not targeted at any particular country, but would incorporate intelligence community identification of the threat posed or potentially posed by any given country for any particular transaction.

In assessing companies, we would determine if the company was a state-owned enterprise, whether the company had been created for the specific deal, or if the company or its ownership was reliable and stable. To assess commodities and technology, we would assess criticality to DoD weapons systems, both current and future, how cutting edge the technology was, whether the technology was already globally available, and what the impact of a supply chain disruption would be.

Co-location cases, again, cases in which land or facilities near critical military training and test ranges was being purchased, became more prevalent over time. In these cases, we would assess what activities were taking place at a given location and whether the purchasing party would be able to observe or impact those activities.

If the DoD assessment raised a concern over any one of the C's, DoD would perform a deeper assessment of a given transaction. If we had concerns with two or more C's, my experience was that such cases were likely headed to mitigation of some kind or a recommendation to block. As I noted, current CFIUS and agency authorities allowed us to properly adjudicate cases regardless of whether the country involved, the company involved, the commodity or technology involved, or co-location was the issue.

Before moving onto areas where I believe CFIUS authorities need to be expanded or clarified, I do want to compliment the Treasury staff and the intelligence community for

the support that they provided to CFIUS. The Treasury staff worked very closely with the DoD, which I believe had co-leadership on most of the difficult cases. Treasury did an excellent job of making the process more efficient during my time as a Committee member, and they were always willing to adjust the internal process as the cases grew in complexity. The intelligence community provided much needed background on cases and they also altered their process to shorten timelines and provide additional detail, again as the cases grew in complexity.

I'd like to now turn to areas where I believe CFIUS needs expanded authorities. I recognize there are proposals currently being reviewed by this Congress. My comments are not based on any specific legislation, but rather, they are based on my CFIUS experience.

The first area I believe CFIUS needs to have increased jurisdiction over is Joint Ventures. Some Joint Ventures, in which companies form partnerships with other companies and in which ownership of the original company does not change, may put national security at risk through technology or intellectual property transfer. While I'm sure the vast majority of Joint Ventures do not threaten national security, the same three C's plus one framework I applied to CFIUS acquisition transactions involving foreign companies should be applied to Joint Venture transactions.

Coverage over entities in bankruptcy is another area where I believe we need to expand CFIUS authorities. Bankruptcies of US companies, especially those involved in futuristic or cutting edge technologies, could end in the sale of technology or intellectual property assets to countries or companies of concern. Again, CFIUS should be allowed to review these transactions, and if required, allowed to mitigate or block them.

The final area I believe we need to assess with regard to CFIUS authorities is what I called "connecting the dots." Under current CFIUS authorities, each transaction is reviewed separately, which generally works. However, during my time as a CFIUS representative, we noticed trends in which specific countries, and many times, companies, were engaged in multiple transactions involving segments for industry. These trends usually mirrored a country's stated goal of increasing its own capacity in a given industry segment. Most times, the companies and technologies being purchased were relatively small, not state-of-the-art, and not critical to national security. However, just as in merger and acquisition anti-trust assessments, there comes a point when too much of a particular segment of industry is under foreign control. In addition, while these small, not state-of-the-art companies may in and of themselves not be critical to national security, they may play a role in the supply chain of more critical companies. Control of multiple entities in a particular industry segment may also allow the mapping of the supply chain for the broader industry. Again, this may put national security at risk and should be assessed. I don't know what the tipping point for too much outside control of an industry segment is, and it likely varies by industry and by technology, but I believe that CFIUS must be given authority to assess trend analysis and weigh in on transactions based on that analysis when necessary.

The last area I would like to address is resources. The reality is that just to handle, manage, and mitigate the cases in the current workload, CFIUS needs more resources. The cases coming before the Committee are growing in their complexity, and I firmly believe that certain countries are actually testing the CFIUS process and seeking the gaps to overcome CFIUS. Resources are needed to adequately perform the due diligence on the cases that come before CFIUS in the time frames required by the CFIUS legislation. If CFIUS authorities are expanded in the ways I have outlined above or as outlined in proposed CFIUS legislation, CFIUS, both centrally and within each CFIUS member agency, will need more resources to process cases. Resources are also needed to adequately assess unfiled transactions, potentially the lower part of an iceberg of CFIUS-related threats to national security.

CFIUS also needs resources to perform mitigation oversight. As cases have grown in their complexity, mitigation agreements have also grown in complexity. To expect these agreements to be enforced from within existing staff resources is simply not realistic. Even when companies pay for the mitigation, the Federal government oversight is still required and must be resourced. I make this plea not as someone who currently has responsibility for managing stretched federal government resources, but as a private citizen with deep experience in this area and concern for our national security.

I thank the Committee for holding this hearing. This is a critical topic for continuing the long-term viability of our technological superiority – and technological superiority remains one of the foundations for our military capability. I look forward to your questions.

Written testimony of

Ambassador Robert M. Kimmitt
Former Deputy Secretary and General Counsel of the U.S. Treasury

Before the Subcommittee on Monetary Policy and Trade
of the
Committee on Financial Services
United States House of Representatives

Foreign Direct Investment: Striking the Balance

December 14, 2017

Mr. Chairman, Ranking Member Moore, members of the Subcommittee,

Thank you for your invitation to discuss today's important topic. It is a particular pleasure to appear with my distinguished fellow panel members.

In my capacity as a former government official, I would like to offer perspective on the Committee on Foreign Investment in the United States (CFIUS). This is one of those rare instances where advancing age, which includes over three decades of work on CFIUS, has some benefits.

My experience with CFIUS began in 1985, when I served as Treasury Department General Counsel under President Ronald Reagan and Secretary James Baker. CFIUS was then governed by its founding Executive Order, signed in 1975 by President Ford because of concern about Saudi petrodollars being recycled to buy American assets.

Later during my service at Treasury, concern had shifted to Japanese purchases, which led to passage in 1988 of the Exon-Florio Amendment to the Defense Production Act, which gave CFIUS its first statutory basis. In 1992, concern about state-owned companies buying sensitive

US technology companies led to passage of the Byrd Amendment, subjecting state-owned acquirers to special scrutiny.

In 2005, I returned to Treasury as Deputy Secretary. After deals involving the Chinese National Overseas Oil Company (CNOOC) and Dubai Ports were blocked by congressional concerns, Congress passed the Foreign Investment and National Security Act of 2007 (FINSA), the governing legislation for today's operations of CFIUS.

Because of growing concern about Chinese investment in the United States, particularly by state-owned enterprises and especially, but not exclusively, in the technology sector, legislation has been proposed by a bipartisan group of legislators led by Senator Cornyn and Congressman Pittenger. While I am not appearing to discuss individual elements of the proposed legislation, I would like to offer some observations that may assist in your deliberations:

- Every public official has a solemn and primary obligation to safeguard US national security. Earlier this year, this Committee, in making the Secretary of the Treasury a statutory member of the National Security Council, recognized that our economic strength is tightly linked to our overall security.

- Any analysis of foreign direct investment (FDI) should begin by recognizing its important contribution to the US economy. My former boss, then Treasury Secretary Baker, described foreign investment as America's economic "ace in the hole," because such investment represented a foreign company's strong vote of confidence in the US market and American workers.

- Nancy McLernon will cover this point far better, but I would note that almost 7 million Americans will receive their paychecks this month from companies headquartered overseas. A full 40% of those workers are in manufacturing jobs, versus 13% in the overall economy. So an FDI job is three times more likely to be in manufacturing, and these jobs pay about 25% more than the economy-wide average. That is why a more open investment policy is integral to US economic success, and I urge President Trump

to join his predecessors, save one, in issuing the traditional US Open Investment Policy statement at the earliest opportunity.

- But in issuing that statement, and in considering the bill before you, it is important to make clear that the US Government must ensure foreign investment does not harm US national security interests. Chinese investment has an appropriately high priority for close scrutiny, because China seeks to compete strategically against the United States in multiple spheres – military, diplomatic, and economic – using all elements of the state, including state-owned enterprises, in that competition. We are also witnessing a greater complexity of proposed deals, specifically those involving companies in the technology sector.

- It is important to note that Exon-Florio provided, and FINSA provides, significant authority to identify and block troublesome Chinese acquisitions. The first acquisition unwound by a President was China National Aero-Technology's stake in Mamco Manufacturing in 1990 under George H.W. Bush. Huawei's acquisition of 3Com did not proceed under George W. Bush. Huawei's acquisition of 3Leaf; Ralls' acquisition of wind farms near a US naval base; and Fujian Grand Chip's attempted acquisition of Aixtron's US assets were blocked by President Obama. And President Trump recently blocked the acquisition of Lattice Semiconductor by a Chinese investment group.

- As you consider new legislation, therefore, I would be sure to address actual gaps in existing authority. There is particular concern that Chinese companies may be using creative legal structures to conclude deals short of ownership or control that could nonetheless impair US national security. I believe this is a very valid area for stricter scrutiny in the United States. I would be careful, however, about extending CFIUS's reach to transactions occurring outside the United States.

- This comment raises a very important point: CFIUS is intended to give the President an exceptional authority to protect the United States, without, however, superseding or substituting for important authorities in other statutes. So, for example, if a joint venture

abroad raises concerns about technology transfer or compromise, the export control regime and authority under the Export Administration Regulations (EAR) or International Traffic in Arms Regulations (ITAR) should be the first line of defense. Today, when others in the interagency community cannot resolve contentious issues under their authority, those issues are often adjudicated in CFIUS, counter to the law's admonition that CFIUS be an authority of exceptional rather than primary resort. Both Alan Estevez and Kevin Wolf, who have more relevant and more recent export control experience than I, will also have important perspectives on this point.

- This leads me to the view that the greatest problem facing CFIUS today is not a lack of authority, though additional authority is warranted, but rather a lack of resources. As cases filed before CFIUS climb to 250 this year, and with the prospect that CFIUS agencies led by Treasury could be involved next year in a time-consuming legislative and regulatory implementation exercise, I think the increase in workload may begin to delay jobs-producing investments that do not raise national security concerns. It will also leave less time for Treasury to engage in important pre-deal discussions with investors looking for guidance on how best to identify opportunities that do not raise security concerns. The draft bill recognizes this resource challenge, and I urge that matching requirements to resources be a central point in your further deliberations.

- Today's hearing and your future actions are also being watched closely overseas. Germany has already tightened its investment screening mechanism; Britain is considering doing the same; and, of concern, the European Commission (EC) in Brussels is establishing an investment review mechanism – even though under European law the Commission has no authority or jurisdiction on security matters. So the new EC review may become a political screening process that could create a new barrier to US investment into that important market of over 300 million consumers.

- These and similar developments around the world lead me today to be more concerned about investment protectionism than trade protectionism. If we want to continue to grow well-paying FDI jobs in the United States, we must send a clear message that we are open

to investment except in those instances where a CFIUS process focused squarely on national security determines an investment must be blocked. I know you will strive to strike that important balance.

Thank you for your kind attention. I look forward to your questions and my fellow panelists' presentations.

House Financial Services Committee
Subcommittee on Monetary Policy and Trade
Hearing on "Examining the Operations of the Committee on Foreign Investment in the United States"
Testimony of Nancy McLernon
President & CEO, Organization for International Investment
December 14, 2017

Chairman Barr, Ranking Member Moore, and other distinguished members of the Subcommittee, thank you for the invitation to testify this morning. My name is Nancy McLernon and I serve as the President and CEO of the Organization for International Investment (OFII). OFII is the only business association exclusively comprised of U.S. subsidiaries of foreign companies. Our mission is to ensure that the United States remains the most attractive destination for foreign direct investment (FDI). As such, we advocate for non-discriminatory treatment in U.S. law and regulation for these firms and the millions of Americans they employ. Given our unique membership, I believe OFII is well positioned to be a constructive voice in your deliberations moving forward as our companies are some of the Committee on Foreign Investment in the United States' (CFIUS) primary users.

The inbound business community applauds efforts of this Subcommittee to carefully examine the current operations of CFIUS and efforts by Senator Cornyn and Representative Pittenger, among others, to reform and modernize CFIUS. Working to safeguard the United States from those who would exploit this country's open economy to do us harm is of paramount importance. We welcome the recognition that as part of this legislative undertaking, it is critically important to truly focus on national security and not hinder the economic openness that has propelled our nation's prosperity.

Impact of Foreign Direct Investment in the United States

The impact of FDI in the United States is tremendously beneficial. International companies employ 6.8 million workers in the United States – including 20 percent of the U.S. manufacturing workforce.[1] In fact, between 2010 and 2014, two thirds of all new manufacturing jobs that were created can be attributed to FDI.[2] Across the country, U.S. workers at FDI companies earn 24 percent higher compensation than the economy-wide average.[3] In addition, these companies engage in high levels of research and development (R&D), accounting for 16 percent of all R&D performed by U.S. companies.[4] They also make extensive capital investments in new facilities and equipment totaling nearly $100 billion dollars annually and produce 23 percent of U.S. exports – that's nearly a billion dollars of exports every single day.[5] Further, international companies fuel local growth by purchasing hundreds of billions of dollars

[1] Department of Commerce Bureau of Economic Analysis, Survey of Current Business Activities of U.S. Affiliates of Foreign Multinational Enterprises, (Washington, DC: Aug. 2017).
[2] Lesley Wroughton and Howard Schneider, "'Bad' Foreign Firms Drive U.S. Manufacturing Jobs Revival," Reuters, (June 2017).
[3] Department of Commerce Bureau of Economic Analysis, Survey of Current Business Activities of U.S. Affiliates of Foreign Multinational Enterprises, (Washington, DC: Aug. 2017).
[4] Ibid.
[5] Ibid.

in goods and services from local U.S. suppliers – creating huge opportunities for America's small businesses.[6]

Historically, mergers and acquisitions (M&A) make up more than 80 percent of FDI activity in the United States. This is true in most developed countries. Therefore, most of the benefits derived from FDI is attributable to M&A activity. Given this reality, it is critical we ensure the environment for cross-border M&A remains open. Importantly, the vast majority of FDI entering the United States is in industries totally unrelated to U.S. national security.

For example, L'Oréal USA leads America's beauty industry in part because of their strategic acquisitions of local brands such as Kiehl's and Urban Decay. These acquisitions have expanded L'Oréal's footprint in the United States to include research, manufacturing and distribution facilities across 13 states including Arkansas, California, Florida, Kentucky, New Jersey, Ohio, Texas and Washington with a workforce of more than 11,000 employees.

International companies are also closely tied to their communities. They provide world-class workforce training and help strengthen the communities in which they sustainably operate. For example, Toyota, whose Kentucky plant is their largest manufacturing facility in the world, is applying its manufacturing know-how to help other manufacturers, non-profits, community organizations, and government entities develop better ways of doing their day-to-day work. Through an organization called the Toyota Production System Support Center (or TSSC), Toyota has helped Children's Hospitals reduce infection rates within neonatal intensive care units. As a result, infections have decreased by approximately 80 percent.

America has long been the preferred destination for FDI because of our economy, infrastructure, rule of law and workforce. However, competition to attract and retain FDI has never been stronger, providing companies with an unprecedented array of options when looking to expand into new markets around the world. Unfortunately, over the past few years, the United States has seen its share of FDI dramatically decline, from 37 percent in 2000 to just 24 percent in 2016.[7] Therefore, it is critically important to implement policies that make the United States more attractive for international companies – including modernizing the CFIUS process.

OFII Support for Reforming CFIUS

OFII has strongly supported the efforts of the Financial Services Committee and others to ensure America's open economy does not hamper U.S. national security. OFII members have extensive experience with national security reviews conducted by CFIUS, as authorized under Section 721 of the Defense Production Act of 1950.

Ten years after Congress enacted the Foreign Investment and National Security Act of 2007 (FINSA), which extensively amended Section 721, it is timely for this Subcommittee to evaluate how Congress's vision for Section 721 has worked, and whether the tools Congress provided to address national security concerns arising from foreign investment remain adequate for our current economic and security environment.

---

[6] OFII, Global Investment Provides the Jobs We Need, (Washington, DC: June 2016), 12.
[7] UNCTAD, World Investment Report 2017.

From the perspective of OFII members, the Section 721 process has largely achieved FINSA's objectives of enabling thorough, nonpoliticized reviews cross-border mergers and acquisitions for possible national security concerns. FINSA, the result of extensive deliberations in Congress, laid the foundation for success. Importantly, in 2008, CFIUS engaged in an equally thoughtful rulemaking process to implement FINSA. The resulting regulations carefully capture the balance that Congress sought, providing helpful guidance on the kind of transactions that are within the purview of CFIUS and the wide range of factors relevant to national security assessments.

CFIUS' annual reports over the past decade generally show that the CFIUS process has functioned as expected. The most recent report, for 2015, indicates that once again, CFIUS cleared more than half of all filed transactions during the initial review period. Only 11 cases (8%) resulted in mitigation agreements, with another 13 notices (9%) being withdrawn.[8] These numbers are generally in line with those from prior years, and indicate that CFIUS has indeed focused its resources on transactions that warrant inquiry.

A critical factor in the attraction of the United States to foreign investors is our country's commitment to the rule of law, and the predictability and stability that regulatory consistency can provide. OFII believes that CFIUS has administered Section 721 largely to this end.

Recent Developments

Although the CFIUS reports for the past two years will not be available for some time, based on publicly available information, and the anecdotal experience of OFII members, it seems clear that the CFIUS process is under stress and that the prior years' pattern of CFIUS outcomes is changing. There appear to be more investigations and mitigation agreements, withdrawals of cases, and lengthening periods for resolution of cases. CFIUS's interpretations of its regulations has also become more unpredictable.

Many factors contribute to this period of uncertainty. Robust investment activity is occurring in the tech sector, and others, where national security concerns particularly reside. New commercial innovations, such as mining of big data, present complex new issues for assessment.

Without doubt, the nature and increased volume of outbound investment from China in recent years has influenced the administration of Section 721 by CFIUS and, more profoundly, the calculation of national security risk. OFII believes that as CFIUS adapts to new investment trends and challenges, it is especially critical to maintain a balanced, reasoned approach to risk assessment.

Supporting FDI With an Efficient and Effective CFIUS Process

As Congress considers proposals to reform CFIUS, I believe it is critical to remember the linkage between economic security and national security. As I referenced earlier, the United States is already experiencing a decline in its share of FDI. Unnecessary changes to the process will only further decrease U.S. competitiveness for cross-border investment.

Our member companies report that, although CFIUS staff continue to impress with their long hours and attention to the unique circumstances presented by each case, resource constraints are

[8] CFIUS, Annual Report to Congress CY2015, (Sept. 2017), 1-2.

straining the CFIUS' ability to handle its current workload. The demands of new cases are compounded by the requirements of monitoring the increasing number of mitigation agreements.

OFII thus encourages Congress to review the current organization and funding of CFIUS activities. In addition, Congress and CFIUS should explore other ways of administratively easing the strain. One would be a "fast track" option that would allow for expedited resolution of transactions that lack the complexity or controversy that lead to delayed processing and systemic bottlenecks. Such delays in processing ultimately impact business and investment decisions. Another area for study is possible efficiencies in the oversight of mitigation agreements.

CFIUS should not be viewed as the panacea for espionage or trade imbalances. Illegal efforts to acquire U.S. technology, such as industrial espionage and cyber hacking, should be aggressively addressed, but such efforts are outside the scope and ability of CFIUS. It would be a critical error to shoehorn larger espionage concerns into the CFIUS mandate. Likewise, CFIUS should not become a way to address concerns that have been expressed concerning trade imbalances. If trade reciprocity is viewed to be a problem, Congress should work with the Administration to explore, utilize and modernize other tools at its disposal to alleviate those perceived concerns.

FDI plays a significant role in growing America's economy and creating the jobs our country needs. International companies invest in our local communities for the long-term. Efforts to reform CFIUS should be undertaken carefully and deliberately. Ensuring fairness, predictability and efficiency in national security reviews must remain tenets of the CFIUS process.

Once again, I thank the Chairman for the invitation to join the Subcommittee this morning and I look forward to answering your questions.

COUNCIL *on*
FOREIGN
RELATIONS

December 12, 2017

Chinese Technology Development and Acquisition Strategy and the U.S Response

Prepared statement by
Adam Segal
Ira A. Lipman Chair in Emerging Technologies and National Security and Director of the Digital and Cyberspace Policy Program
Council on Foreign Relations

Before the
House Committee on Financial Services,
Monetary Policy and Trade Subcommittee
United States House of Representatives
1st Session, *115*th Congress

Hearing on Examining the Operations of the Committee on Foreign Investment in the United States (CFIUS)

Introduction

Chairman Barr, Ranking Member Moore, and members of the committee, thank you for the opportunity to testify on this important subject.

While the openness of U.S markets and science and technology (S&T) system is central to economic and national security, it is also a threat to those same interests. China in particular has benefited from access to U.S. universities, companies, and markets, and the diffusion of technologies and knowledge from the United States and other advanced economies has played a role in the acceleration of the modernization of the People's Liberation Army.

The challenge for policy makers is twofold. First, China's strategy to develop, acquire, and diffuse technology for economic and security interests is multifaceted involving investments in research and development, industrial policy, protection of intellectual property, talent development, and foreign acquisitions. The U.S. response therefore must be similarly broad. Any policy, say reform of the Committee on Foreign Investment in the United States (CFIUS) or export control laws, is necessary but not sufficient, and the United State must also address Chinese techno-nationalism more broadly.

Second, policy makers must adopt measures to block the flow of critical technologies to potential adversaries while not inflicting self-harm. While there are tight links between economic and national security, policies should be narrowly focused on preventing the acquisition of technologies that would threaten the U.S. military edge, not broader economic competitiveness writ large. This is made more difficult by three factors: globalization of science and technology; the tight integration of the U.S. and Chinese S&T systems; and the dual-use nature of many frontier technologies, especially artificial intelligence (AI).

China's science and technology strategy

The United States is still the world leader in science and technology, but others are increasing their capabilities rapidly. A report from the UK Royal Society describes the situation as an "increasingly multipolar scientific world, in which the distribution of scientific activity is concentrated in a number of widely dispersed hubs."[1] Middle income countries—including India, Brazil, and China—have expanded their expenditures on R&D, increasing their contribution to world R&D spending from 40.8 percent in 2007 to 47.3 percent in 2013.[2]

China's goals in science and technology are particularly noteworthy. The 2006 National Medium- and Long-Term Plan for the Development of Science and Technology states China's goal of becoming an "innovative nation" by 2020 and a "global scientific power" by 2050.[3] Beijing sees technological innovation as central to ensuring that China does not remain the factory of the world and moves up the value chain—that it shifts from "made in China" to "invented in China." Chinese policy makers also have a long history of techno-nationalism and want to reduce their technological dependence on advanced economies, especially the United States and Japan. In addition, the Chinese leadership sees a tight link between technological and military strength. In an address to military delegates at the March 2017 meeting of the People's Congress, President Xi Jinping noted that science and technology were "key to military upgrading" and called for "a greater sense of urgency to push for science and technology innovation."[4]

China's investment in R&D has grown by 20 percent a year since 1999.[5] R&D spending is now approximately $233 billion, 2.1 percent of GDP, and 20 percent of total world R&D expenditure.[6] China is also now the world's largest producer of undergraduates with science and engineering degrees, and Chinese scientists are writing a large number of scientific papers, a growing number of which are well-cited. In 1996, the United States published more than ten times as many scientific research papers as China. China is now the second largest producer of scientific papers after the United States, and has shown large gains in computer science, engineering, and AI. Ethnic Chinese authors, for example, account for 43 percent of the top 100 AI journals and conferences.[7]

Science and technology is front and center in the 13th Five-Year Plan (2016-2020). Science and technology development is discussed first in the plan and for longer than any other subject.[8] This broad plan is being fleshed out through industrial policies designed to raise China's innovation capabilities, three of the most important being: an attempt to build an indigenous semiconductor industry; "Made in China 2025"; and the "Next-Generation Artificial Intelligence Development Plan." All are strategic initiatives aimed at facilitating China's dominance in various high-tech spaces.

China's 2014 "IC Promotion Guidelines" involves new backing for semiconductors, with reported investments between $100 and $150 billion in public and private funds. The goal is to close the gap with other countries in the design, fabrication and packaging of chips of all types by 2030; to have Chines firms produce 70 percent of the chips consumed by Chinese industry; and to end dependence on foreign supplies. Policy makers have likened Chinese dependence on foreign chips to its need for foreign oil; China imported $228 billion of integrated circuits in 2016. The government provides capital subsidies to domestic firms, and to foreign firms who locate in China, as well as encourages domestic consumers to purchase only from Chinese suppliers.

"Made in China 2025" sets out ambitious targets for upgrading China's aging manufacturing base through smart manufacturing. This includes integrating automation, smart sensors, and Internet of Things (IoT) devices into Chinese industry. Borrowing from Germany's 'Industry 4.0,' China sees an opportunity to use industrial policies to dominate high value-added industrial sectors like aviation, integrated circuits, next-generation information technology, robotics, new energy vehicles, and biopharmaceuticals. The plan offers low-interest loans from state-owned investment funds and development banks; assistance in buying foreign competitors; and extensive research subsidies.[9]

China's "Next-Generation Artificial Intelligence Development Plan" provides a roadmap for China to dominate the emerging artificial intelligence space and encourage broad adoption of AI across the economy and society. China currently trails the U.S. in terms of producing top-rated AI research and patents. But China has at least three advantages: huge data sets; a permissive regulatory environment with very little concern for privacy; and significant government support and investment.

The Next-Generation Artificial Intelligence Development Plan" aims to turn China's AI industry into a "world leader' worth RMB 400 billion ($60 billion) by 2025 and a 'premier innovation center' worth RMB 1 trillion by 2030 ($150 billion). So far, China's Ministry of Science and Technology has established an AI advisory committee with a mix of state scientists and private sector leaders and has enlisted China's largest tech companies to join an 'AI national team' and build "open innovation platforms" for several applications of AI.[10] Cooperation with private companies is a prominent part of China's AI push, with several Chinese companies designated as national champions to close the gap between China and the U.S. In February2017, the National Development and Reform Commission commissioned Baidu to build a national laboratory for deep learning in partnership with two Chinese universities.[11]

Inward investment regime

Access to the Chinese market has often been predicated on the transfer of technologies. Foreign firms are often pressured to license technology to Chinese partners or establish R&D centers within China. General Motors, for example, was reportedly precluded from receiving purchase subsidies for the Volt, its electric hybrid car, until it transferred engineering knowledge from its three main technologies (electric motors, complex electronic controls, and power storage devices) to a joint venture with a Chinese automaker.[12] In April 2010, Beijing ordered high-tech companies to turn over the encryption codes to their smart cards, Internet routers, and other technology products in order to be included in the government procurement catalog. [13] Firms are also often forced into joint ventures, frequently with state-owned actors. These partnerships regularly result in inadvertent technology transfer as engineers and managers work together, or more directly from the outright theft of intellectual property.

China's longstanding willingness to turn a blind eye to intellectual property theft has also resulted in widespread technology transfer. The problem has been especially prominent in software, where Microsoft estimates that 95 percent of its Office software and 80 percent of Windows operating system operating in China are pirated. 80 percent of Chinese government agencies are suspected of running illegal copies of Microsoft and other foreign software. [14] While the enforcement of IP law has recently improved, over the long term Chinese firms benefited from not having to invest in their own R&D and not paying licensing or royalty fees.

Foreign acquisitions

While China's innovation strategy emphasizes "indigenous innovation", it also encourages Chinese companies to acquire core technologies and know-how abroad as a means of catching up or leapfrogging the competition. There are a number of channels, both legal and illegal, for Beijing to acquire new technology.

Foreign purchases have played a large role in the semiconductor strategy. Chinese investment in the United States in 2016 was $45.6 billion, and Chinese firms have, according to estimates from the Rhodium Group, made about $34 billion in bids for U.S. semiconductor companies since 2015.[15] Tsinghua Unigroup emerged from relative obscurity to purchase two Chinese firms for $2.6 billion. It bought a 51 percent stake in H3C, a Hong Kong subsidiary of Hewlett-Packard that makes data-networking equipment, for $2.3 billion. Bids for Micron, a big American maker of DRAM (type memory chips used to store data on desktop computers and servers), SK Hynix, a South Korean DRAM manufacturer, and Western Digital failed because of political opposition.[16] Other Chinese entities have also faced political opposition. In 2016, CFIUS rejected the sale of Aixtron SE of Germany to China's Fujian Grand Chip Investment Fund. In September 2017, President Trump blocked Canyon Bridge Capital Partners LLC, a China-backed buyout fund, from acquiring Lattice Semiconductor Corp for $1.3 billion.

In other instances, China has purchased portions of large semiconductor companies, perhaps to stay under the threshold for investigation. Jianguang Asset Management Co. Ltd. (JAC Capital), for example, bought NXP's RF Power business for $1.8 billion.[17] The sources of Chinese investment are opaque. Unigroup, a commercial entity spun off from Tsinghua University, appears to receive significant financial support from the government. The owner of Fujian Grand Chip Investment Fund, for example, is a private businessperson, Liu Zhendong. But Sino IC Leasing, a subsidiary of the National IC Fund, offered to provide a loan of 500 million to make the Aixtron deal possible. Moreover, in the months before Aixtron sought new investors, its share price tumbled after Fujian-based San'an Optoelectronics cancelled a large order of machines in late 2015. A report from the Mercator Institute of China Studies suggests a close relations between San'an, Fujian Grand Chip, and the National IC Fund. The parent company of San'an Optoelectronics, the San'an group, owns shares in Sino IC Leasing.[18] This lack of transparency makes it difficult to differentiate between economic and strategic motivations for a purchase.

In the face of this growing scrutiny, Chinese entities appear to be pursuing other means of acquiring technology in order to circumvent oversight. According to a 2017 report from the Defense Innovation Unit Experimental, China is participating in an increasing number of venture deals, about 10 percent of all venture deals in 2015 up from a 5 percent average participation rate during 2010-2016. Beijing is especially active in the areas of artificial intelligence, autonomous vehicles, augmented/virtual reality, robotics, and blockchain technology.

Baidu, for example, is partnering with Comet Labs, a San Francisco-based fund specializing in machine intelligence. In August 2016, Baidu and Ford jointly invested $150 million in Velodyne, a maker of LiDAR sensors, which are an important component of self-driving car technology. The company began developing sensors for driverless cars after participating in a DARPA competition in 2005 and has since sold its technology to the Navy for unmanned surface vehicles.[19] In April 2016, state-backed Haiyin Capital made a minority investment in Neurala, which is developing AI technology that can automate self-driving cars, robots, and drones.[20] According to the *New York Times*, Neurala's CEO had been in talks with the U.S. Air Force about a partnership, but grew frustrated by the slow pace at which talks progressed. A report from Defense Group Inc. stated that Huiyin's investment in Neurala creates uncertainty over China's access to the company's source code and whether Neurala's technology is secure for U.S. end-users. [21]

Cyber and industrial espionage

China also acquires foreign technology through cyber and industrial espionage. During this decade, Google, Nasdaq, DuPont, Johnson & Johnson, General Electric, RSA, and at least a dozen others have had proprietary information stolen by Chinese-based hackers. A 2013 private commission, chaired by Dennis Blair, former director of national intelligence, and Jon Huntsman, former ambassador to China, argued that the annual "losses are likely to be comparable to the current annual level of U.S. exports to Asia—$300 billion." Cybersecurity companies noted a significant decline in Chinese activity after the 2015 agreement between President Obama and President Xi, in which both sides agreed not to hack each other's private companies for commercial gain.

4

Recent reporting suggests, however, that China is pushing the envelope, going after technologies that are dual-use, and so might not be covered by the agreement, as well as some civil society groups.

In the physical world, Chinese nationals have been charged in the theft of radiation-hardened microchips, precision navigation devices, the processes for high-volume manufacturing of chips used to light and electrify flat-screen TVs and smartphones, and other technologies. In addition, according to a recent report for the U.S.-China Economic and Security Review Commission, the theft of American technology is often conducted through China's science and technology institutes and industrial enterprises. [22] The "key modality is no longer the spy," according to Jim Richberg, former deputy national counterintelligence executive, "but the businessman, student, or academic." [23]

National security implications

Science and technology diffusion has and will continue to improve Chinese military capabilities. Shifting research centers to China and developing collaborative business relations with Chinese companies involves American institutions in the diffusion process, inadvertently speeding Beijing's military modernization. In China, the shipping and telecommunications sectors have made steady improvements in R&D and production through their engagement with the international economy and these technological capacities have been converted into new military capabilities.[24] The 2011 report from the U.S.-China Economic and Security Review Commission argues that U.S. aerospace companies may have unknowingly assisted Chinese military modernization.

The newest wave of Chinese investment in sensitive technologies such as robotics, AI, and sensors is a further threat to the U.S. technological edge. Some of these technologies will inevitably end up in the hands of enterprises and universities with tight links to the PLA. Moreover, Chinese investment in high-tech firms could prevent U.S. government or military investment and cooperation with those same companies.[25]

In addition, Chinese leaders are intent on building a system that allows the military to take advantages of gains in the civilian economy. Civil-military fusion [军民融合 *junmin ronghe*] is a pillar of Chinese military modernization and an effort to bolster the country's innovation system for advanced dual-use technologies in industries like aviation, aerospace, and information technology. Introduced by former President Hu Jintao in 2009, the effort to bridge the gap between the civilian industrial base and the military has intensified under President Xi Jinping. Within his first year in office, the Central Committee voted to elevate civil-military fusion to a national strategy, and in January 2017 Xi created the Central Commission for Integrated Military and Civilian Development, a new high-level decision making and coordination body for civil-military fusion efforts.[26]

Civil-military fusion plays a prominent role in both "Made in China 2025" and the "Next-Generation Artificial Intelligence Development Plan." Emerging technology like AI, drones, robotics, and big data are already blurring the line between technology intended for military and commercial purposes; China's strategy has been to treat military and commercial technological developments as two-sides of the same coin. For example, prominent AI researchers like Le Deyi, who is the head of the China Association for Artificial Intelligence, participate in research with commercial enterprises and hold rank in the People's Liberation Army.

Policy challenges

Any attempt to prevent technology flowing to China and improving military capabilities is complicated by at least three factors. First, as noted above, innovation is increasingly global, and there are few technologies that the U.S. monopolizes. Even in artificial intelligence, which seems to be shaping up as a two-way race between

the United States and China, there are clusters of excellence in the UK, Canada, and Israel. Any U.S policy will have to be sensitive to the fact that there are other sources of technology.

Second, the border between "American" and "Chinese" science and technology is no longer as sharp as international R&D networks and business collaborations expand. China-based scholars, for example, choose to coauthor with U.S. colleagues more frequently with those from other countries; nearly 40 percent of China's science and engineering publications in international journals had U.S.-based coauthors. The information technology sector is particularly interconnected, stretching across the Pacific and involving Chinese, American, and Taiwanese entrepreneurs, designers, managers, and technicians. Research and development in AI is likely to replicate this pattern. A number of high profile researchers like Andrew Ng have moved from U.S. universities and companies to Chinese firms and then back again. As a result of this interconnection, policies designed to prevent the flow of technology or people could have a negative impact on U.S. capabilities.

Finally, the list of purely military technologies that the United States can control has become very narrow. Most of the technologies underlying the AI and robotics revolutions will be dual use. There is, for example, likely very little to distinguish the technology in a self-driving car and a self-driving tank.

Policy recommendations

Given these challenges, three principles should guide U.S. policy making.

First, CFIUS reform should be small part of the U.S. response to Chinese technology development and acquisition. Trade efforts to combat techno-nationalism and remove coercive policies to transfer technology are especially important tools to prevent the uncontrolled diffusion of technology and knowledge to Beijing. A great deal of technology transfer happens under the threshold of CFIUS (or export controls) but under pressure from and in return for market access to China.

In addition, some of the worry about China's rise as a science and technology power is compounded by a fear that the United States has been distracted, neglecting science and underfunding basic research. Several top science posts in the White House remain vacant. The president's budget request includes significant cuts of the budgets of the National Science Foundation, National Institute of Health, and Environmental Protection Agency, and the new tax law has a negative impact on science, taxing tuition waivers used by graduate students in science, technology, and mathematics.

Second, unilateral action will be of limited use. China is expanding its science and technology partnerships with Europe, Israel, India and others. Unless Washington and its friends agree to a similar set of technologies to control, Beijing will easily elude U.S. policy. Past attempts to control dual-use technologies do not provide a great deal confidence, however, that the United States and its partners can create an effective framework for the next generation of innovation.

Third, for any reform effort to succeed, CFIUS will require greater capacity. It will need more capacity to handle new investigations on top of what is already a large volume of cases. It will need more capacity to discern the sources of Chinese investment—who is behind an investment and if the motivation is economic, strategic, or some combination. It will also need new mechanisms to tap into academic and commercial expertise to better understand the development trajectories of frontier technologies and what their relationship to military capacity may be.

[1] "Knowledge, networks and nations: global scientific collaboration in the twenty first century" (Royal Society, London, March 2011) available: http://royalsociety.org/uploadedFiles/Royal_Society_Content/policy/publications/2011/4294976134.pdf.

[2] "UNESCO Science Report: Towards 2030," (UNESCO Publishing: 2016), https://en.unesco.org/unesco_science_report.
[3] "The National Medium- and Long-Term Plan for the Development of Science and Technology (2006-2020)," *State Council*, People's Republic of China, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/China_2006.pdf.
[4] "China's Xi pushes advanced technology for military," *Reuters*, March 12, 2017 https://www.reuters.com/article/us-china-parliament-defence/chinas-xi-pushes-advanced-technology-for-military-idUSKBN16K02V.
[5] Gautam Naik, "China Surpasses Japan in R&D as Powers Shift," *Wall Street Journal*, December 10, 2010, https://www.wsj.com/articles/SB10001424052748703734204576019713917682354.
[6] Reinhilde Veugelers, "China is the world's new science and technology powerhouse," *Bruegel*, August 30, 2017, http://bruegel.org/2017/08/china-is-the-worlds-new-science-and-technology-powerhouse/.
[7] Kai-Fu Lee and Paul Triolo, "China's Artificial Intelligence Revolution: Understanding Beijing's Structural Advantage," *Eurasia Group*, December 2017, https://www.eurasiagroup.net/files/upload/China_Embraces_AI.pdf.
[8] Scott Kennedy and Christopher K. Johnson, "Perfecting China, Inc.: The 13th Five-Year Plan," *Center for Strategic and International Studies*, May 2016, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/160521_Kennedy_PerfectingChinaInc_Web.pdf.
[9] Keith Bradsher and Paul Mozur, "China's Plan to Build Its Own High-Tech Industries Worries Western Businesses," *New York Times*, March 7, 2017 https://www.nytimes.com/2017/03/07/business/china-trade-manufacturing-europe.html
[10] "China recruits Baidu, Alibaba and Tencent to AI 'national team,'" *South China Morning Post*, November 21, 2017, http://www.scmp.com/tech/china-tech/article/2120913/china-recruits-baidu-alibaba-and-tencent-ai-national-team.
[11] "China's first 'deep learning lab' intensifies challenge to US in artificial intelligence race," *South China Morning Post*, February 21, 2017, http://www.scmp.com/tech/china-tech/article/2072692/chinas-first-deep-learning-lab-intensifies-challenge-us-artificial.
[12] Robert D. Atkinson, "Enough is Enough: Confronting Chinese Innovation Mercantilism," *The Information Technology & Innovation Foundation*, February 2012, http://www2.itif.org/2012-enough-enough-chinese-mercantilism.pdf?_ga=2.80672215.1914708704.1513087866-1294095666.1513087866.
[13] Adam Segal, "China's Innovation Wall: Beijing's Push for Homegrown Technology," *Foreign Affairs*, September 28, 2010, http://www.foreignaffairs.com/articles/66753/adam-segal/chinas-innovation-wall.
[14] Enough is Enough: Confronting Chinese Innovation Mercantilism
[15] Bob Davis and Eva Dou, "China's Next Target: U.S. Microchip Hegemony," *Wall Street Journal*, July 27, 2017, https://www.wsj.com/articles/chinas-next-target-u-s-microchip-hegemony-1501168303.
[16] "Chips on their shoulders," *The Economist*, January 23, 2016, https://www.economist.com/news/business/21688871-china-wants-become-superpower-semiconductors-and-plans-spend-colossal-sums.
[17] Junko Yoshida, Lurking Behind Every M&A Is China, *EE Times*, December 13, 2016, https://www.eetimes.com/document.asp?doc_id=1330969.
[18] "Made in China: The making of a high-tech superpower and consequences for industrial countries," *Mercator Institute for China Studies*, December 2016, https://www.merics.org/fileadmin/user_upload/downloads/MPOC/MPOC_Made_in_China_2025/MPOC_No.2_MadeinChina_2025.pdf.
[19] Evan Ackerman, "Ford and Baidu Invest $150 Million in Velodyne for Affordable Lidar for Self-Driving Cars," *IEEE Spectrum*, August 17, 2016, https://spectrum.ieee.org/cars-that-think/transportation/sensors/ford-and-baidu-invest-150-million-in-velodyne-for-affordable-automotive-lidar; Paul Mozur and Jane Perlez, "China Tech Investment Flying Under the Radar, Pentagon Warns," New York Times, April 7, 2017, https://www.nytimes.com/2017/04/07/business/china-defense-start-ups-pentagon-technology.html?_r=1.

[20] Hiawatha Bray, "Boston firm's artificial intelligence technology may have broader applications," Boston Globe, August 14, 2017, https://www.bostonglobe.com/business/2017/08/14/boston-startup-builds-mobile-brains/CJcreIjWZRv0caynAK1DWO/story.html.

[21] Defense Group Inc. "China's Industrial and Military Robotics Development," *U.S.-China Economic and Security Review Commission*, October 2016, Pg, 105, available at: https://www.uscc.gov/sites/default/files/Research/DGI_China%27s%20Industrial%20and%20Military%20Robotics%20Development.pdf.

[22] "China's Program for Science and Technology Modernization: Implications for American Competitiveness," Prepared for The U.S.-China Economic and Security Review Commission, January 2011, https://www.uscc.gov/Research/china%E2%80%99s-program-science-and-technology-modernization-implications-american-competitiveness.

[23] Jim Richberg, "The Counterintelligence Implications of Deemed Export Control," Workshop on the Globalization of the University and Deemed Export Policy, Oak Ridge Center for Advanced Studies, March 6–7, 2006.

[24] Evan S. Medeiros, Roger Cliff, Keith Crane, James C. Mulvenon, "A New Direction for China's Defense Industry," *RAND*, https://www.rand.org/pubs/monographs/MG334.html.

[25] Chinese Investment in Critical U.S. Technology: Risks to U.S. Security Interests: Insights from a CFR Workshop, October 16, 2017, https://www.cfr.org/report/chinese-investment-critical-us-technology-risks-us-security-interests

[26] Xi to head central commission for integrated military, civilian development," *Xinhua*, January 22, 2017, http://news.xinhuanet.com/english/2017-01/22/c_136004750.htm.

United States House of Representatives
Committee on Financial Services
Subcommittee on Monetary Policy and Trade

Examining the Operations of the Committee on Foreign Investment in the United States (CFIUS)

Opening Remarks of The Honorable Kevin J. Wolf
Partner, Akin Gump Strauss Hauer & Feld LLP
Former Assistant Secretary of Commerce for Export Administration (2010-2017)

December 14, 2017

Chairman, Ranking Member, and other distinguished members of the subcommittee. Thank you for convening this hearing and for inviting me to testify on this important national security topic.

For nearly 25 years in both the private sector and government, I have focused my practice on the law, policy, and administration of export control and related foreign direct investment issues. From 2010 to 2017, I was the Assistant Secretary of Commerce for Export Administration. In this role, I was primarily responsible for the policy and administration of the U.S. dual-use export control system and, as a result of the Export Control Reform effort I helped lead, part of the defense trade system. I was also during this time a Commerce Department representative to the Committee on Foreign Investment in the United States (CFIUS), particularly with respect to cases involving technology transfer issues.

Although I am now a partner at Akin Gump Strauss Hauer & Feld LLP, the views I express today are my own. I am not advocating for or against any potential changes to CFIUS or its legislation on behalf of another. Rather, I am here to answer your questions about how the CFIUS and export controls systems work and how they could or could not address whatever policy issues you would like to discuss. I will not speak about any specific case that was or is before CFIUS.

My fellow panelists have already described the content and scope of CFIUS, so I will get straight to my main point, which is that the CFIUS and export control systems complement each other. CFIUS has the authority to control the transfer of technology of national security concerns, but only if there is a covered transaction, however defined. The export control rules regulate the transfer of specific or general types of technology of national security, foreign policy, and other concerns regardless of whether there is a covered transaction. This means that if concerns arise about specific or general types of technology -- whether as part of a CFIUS review or from any other source -- then the export control system can and should control the technology to the specific destinations, end uses, and end users of concern.

Identifying, describing, and deciding how or whether to control dual-use technologies – that is, technologies that have both benign commercial applications and applications of concern – is inherently complex. The export control system is also complex, but its authority to control the transfer of technology for national security, foreign policy, or other reasons is not limited by the need for a transaction. Moreover, the system is designed to constantly evolve as new threats are identified, new technologies of concern are discovered, and widespread commercialization makes existing controls unnecessary or impossible to implement.

The Export Administration Regulations (EAR), implemented by the Commerce Department's Bureau of Industry and Security (BIS), have the authority to impose such controls in coordination with other departments, primarily Defense, State, and Energy. The descriptions of technology in the regulations can be as broad or as narrow as the national security or foreign policy concerns warrant. They are generally connected to physical commodities, but do not need to be. They could be based on a technology's technical parameters, end uses, or merely just a reference to the name of the technology. After a technology or other item is identified, the controls on its transfer can be tailored in the regulations to apply to the whole world or to specific destinations, end uses, and end users to address specific concerns. The control choice is a function of a national security and foreign policy judgment to be made on a technology-by-technology basis and regardless of the existence or nature of any underlying commercial transaction.

Most of the EAR implement U.S. commitments to one of four multilateral export control regimes. These are groups of roughly 30-40 countries that have generally agreed to control the transfer of missile, nuclear, chemical/biological, military, and other items of common concern in similar ways. The advantage to such controls is that our regime allies impose essentially the same controls on their exporters. However, the process for achieving consensus from the member states can take a long time, and the limited resources and time available to the regimes limit the number of proposals that can be considered in a review cycle. These disadvantages are outweighed by the well-tested conclusion that unilateral controls -- those that only one country imposes -- are generally counterproductive because they create incentives for foreign companies to develop the technology outside of the country's control. In the long run, they only hurt industry in the country imposing the control and do not deny the technology at issue to the destination of concern. Indeed, this is why the multilateral systems were created decades ago.

The imposition of unilateral controls, however, can be an effective short-term technique for regulating the export of unlisted sensitive technology. It is with this thought in mind that in 2012, I and my colleagues at Commerce created a novel tool in the EAR to quickly and unilaterally control emerging and other unlisted technologies that warranted control, so long as the technology was eventually submitted to the relevant regimes to be controlled multilaterally.[1] This is referred to as the "0Y521" series of controls in the

[1] *See* 77 Fed. Reg. 22191 (Apr. 13, 2012).

EAR, which mirrors similar authority in U.S. Munitions List Category XXI in the State Department's International Traffic in Arms Regulations.[2]

There are many additional tools within the EAR to address technology transfer concerns. For example, BIS could, with or without a public notice and comment process, add unilateral controls over types of emerging technologies to the control list and control them with a licensing or notification requirement to specific destinations. If the concern is about specific end users, then controls can be placed on those end users through the Entity List, the Unverified List, or amending the military end-user controls.[3] Another tool is the "is informed" authority. Basically, BIS has the authority to inform an exporter in certain cases that licenses are required to export otherwise uncontrolled technologies and other items to specific destinations or specific end users.[4] If the existing authorities in the EAR are too narrow to address a new concern, then they can be easily amended. If, for example, a policy concern pertains to types of industrial know-how and capabilities that are hard to define as technologies, then the EAR could be amended to impose notification or licensing controls on specific types of services provided to particular end uses (such as for intelligence activities).

The precursor to using any of these tools is, of course, identifying the emerging or other unlisted technologies of concern. Admittedly, the focus of the previous administration's export control reform effort was defense trade. Hundreds of individuals put in thousands of hours over the course of eight years to develop and refine after massive public input from scores of Federal Register notices revisions to controls affecting hundreds of thousands of defense and related items. Although the revised control lists (intentionally) require constant tweaking, we made the system significantly better and enhanced our national security as a result.

Whether as part of CFIUS reforms, a new export control reform effort focused on dual-use technologies, or just day-to-day good government, there should be a regular, robust, and creative whole-of-government effort, working closely with industry and our allies, to identify technologies that, for national security or foreign policy reasons, warrant control or decontrol. This is already done as part of the regular annual process to propose changes to the multilateral regime controls, but a fair question raised by this hearing is whether a more aggressive, better-resourced effort is needed to analyze novel and emerging unlisted technologies.

In addition, existing export control law enforcement authorities must be used to ensure that those who are developing or transferring technologies of concern have comprehensive programs to ensure compliance with the rules, regardless of whether the company is domestic or owned by a foreign entity. (The export control rules apply equally to companies in the United States regardless of whether they are foreign-owned. U.S. export control rules also apply to and regulate U.S.-origin technology and

[2] *See* 22 C.F.R. § 121.1.
[3] *See* 15 C.F.R. Part 744.
[4] *See id.*

other items even when they are outside the United States and owned by foreign persons.)

Given my combined CFIUS and export control backgrounds, my opening comments have focused on the technology transfer aspects of CFIUS. Other types of national security issues implicated by foreign direct investment include those that:

(i) have co-location issues (e.g., acquisitions next to military facilities);

(ii) create espionage risks or cybersecurity vulnerabilities;

(iii) could reduce the benefit of U.S. Government technology investments;

(iv) reveal personally identifying information of concern;

(v) create security of supply issues for the Defense Department and other government agencies;

(vi) implicate national security-focused law enforcement equities or activities; or

(vii) create potential exposure for critical infrastructure, such as with the telecommunications or power grids.

Each of these topics warrants its own, separate analysis and commentary when considering possible changes to CFIUS.

In my experience, the existing CFIUS structure, authorities, and internal procedures generally allowed for the resolution of these issues quite well. The Treasury Department was an excellent honest broker and facilitated consensus conclusions – often after lengthy interagency discussion and always with the terrific support from the intelligence community. The agencies were always respectful of the need for a whole-of-government decision that accounted for the particular equities and expertise of the other agencies. The career staff were and remain talented, dedicated public servants.

This last point is key. Given the increase in filings and the increase in more complex cases, the staff was stretched thin when I was there, and I expect they are even more stretched now. They need help. They need more resources, particularly aimed at those involved in monitoring mitigation agreements and studying transactions. I make this polite suggestion not only for their benefit but also for the sake of our national security. I also make the suggestion so that the U.S. remains known as a country that welcomes foreign direct investment with the minimum necessary and quickest possible safe-harbor review burden.

Thus, when considering changes to CFIUS to address national security concerns associated with foreign direct investment (such as those in the list I just mentioned), the questions I would ask are whether

(i) the statutory authority already exists to address the issue through a regulatory or process change;

(ii) another area of law -- such as trade remedies, government contracts, or export controls -- could address the issue more directly and without collateral consequences on foreign investments of less concern; or

(iii) the solution lies simply in more resources to the agencies.

If the answer to any of these questions is "no," then that is the sweet spot for consideration of change to CFIUS legislation.

For each possible change in CFIUS's scope, however, it is vital to weigh the costs. For example, if there is even a small expansion in the scope of CFIUS's review authority, then some companies may be less willing to invest in the United States with the actual or perceived extra burden and time involved in closing a transaction, particularly if there is not a significant expansion in staff. Will investing in other countries become more desirable as a result of any changes? With every expansion in scope, there will be a corresponding and exponential expansion in burdens and costs generally. More regulations lead to more words, which leads to more analyses of those words in novel fact patterns, leading to more filings, more reviews, more mitigation agreements, and on and on. Also, if legislation becomes too prescriptive, then it may limit the ability of the Administration and staff to resolve novel national security issues in a creative way. There were many such situations over the course of the last seven years that I suspect could not have been contemplated by the original drafters of the legislation and the regulations.

National security concerns are, of course, paramount and should guide any final decisions. I absolutely agree with my former Defense Department colleague Alan Estevez that the United States never wants to be in a fair fight and the right, aggressively enforced technology transfer, investment, and other controls are a critical part of maintaining that advantage. I am absolutely not suggesting that they be ignored or traded off for other concerns, but only that they are properly calibrated so as not to create unintended or unnecessary consequences. I am also not suggesting that export controls are the solution to all policy concerns, only that they be used to their fullest possible extent because they can be more tailored. These are intensely difficult decisions to make and cannot be made on the fly without a process and without the input of all those with expertise and an equity in the outcome. Also, the right answer for one type of technology will not be the same for another type of technology.

Finally, when considering any changes to the system, it is important to consider how our allies are controlling or considering controls over foreign direct investment into their

respective countries. Just as the objectives of export controls are furthered by multilateral cooperation, multilateral coordination among allies over foreign direct investment issues could be of common benefit. At a minimum, the US CFIUS process could significantly benefit if there were more authority to share facts and concerns with our allies, after business confidential and classified information issues were addressed.

On export control and CFIUS topics, I have a three-minute, a thirty-minute, a three-hour, and a three-day version. So, I will stop here with these general opening comments and look forward to answering your questions. Thank you again for spending the time to think through this complex and important national security issue.

THE OFFICE OF CONGRESSMAN ROBERT PITTENGER
FOREIGN INVESTMENT RISK REVIEW MODERNIZATION ACT (FIRRMA), H.R. 4311

SUMMARY

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.

STATEMENTS OF SUPPORT FOR CFIUS REFORM

- **U.S.-China Economic and Security Review Commission**: "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."

- **Former Secretary of Commerce Penny Pritzker:** 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 … no government should require technology transfer, joint-venture, or localization as a quid-pro-quo for market access."

- **Secretary of Defense James Mattis**: Stated 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."

- **Dan Coats, Director of National Intelligence:** "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:** Stated 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."

- **Admiral Michael Rogers, Director of the NSA (and Commander of U.S. Cyber Command):** Stated "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."

For more information, please contact the Office of Congressman Robert Pittenger at (202) 225-1976

- **Attorney General Jeff Sessions:** Was asked by Sen. Cornyn whether he supports the effort to modernize and reform the CFIUS process to deal with this threat to national security. "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 [the Cornyn bill] 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."

- **Steven Mnuchin, Secretary of the Treasury**: At a House Financial Services Committee hearing on July 27, 2017, said this about CFIUS reform: "I hope this is something we can definitely do on a bipartisan basis. 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."

- **Admiral Dennis Cutler Blair, former Director of National Intelligence and former commander of U.S. forces in the Pacific region said**: "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."

- **Larry Wortzel. Commissioner, U.S. China Economic and Security Review Commission:** "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."

For More Information

- This legislation mirrors legislation being introduced by Sen. John Cornyn in the Senate.

- Please contact Brian Kennedy, Brian.Kennedy1@mail.house.gov for more information.

For more information, please contact the Office of Congressman Robert Pittenger at (202) 225-1976

Alan F. Estevez

Representative Gwen Moore
Subcommittee on Monetary Policy and Trade
Hearing
Evaluating CFIUS: Challenges Posed by a Changing Global Economy

Questions for the Record

Section 3(a)(5)(B) of the proposed legislation would treat as a covered transaction any transaction involving the contribution by a US critical technology company of intellectual property and associated support. The legislation defines a US critical technology company as any company that produces, trades in, designs, tests, manufactures, services or develops critical technologies. The definition in the proposed legislation of "critical technologies" is very broad and leaves room for further expansion through regulations.

Can each of the witness please answer the following questions:

> The proposed legislation covers contributions of IP by critical technology companies, but as written, the IP could relate to any kind of IP that the company possesses. Shouldn't we focus specifically on the contribution of IP related to critical technologies, and not other kinds of technology that a US critical technology company happens to possess?

I beleive that CFIUS should focus on only the contribution of IP related to critical technologies, not general IP, when reviewing transactions. However, in order for CFIUS to understand what IP companies propose to transfer in an arrangement, such as a joint venture, and to determine whether that IP relates to critical technologies, CFIUS would need to have visibility of the proposed transfer as a part of covered transaction. The CFIUS regulations need to be clear that only transfer of critical technology IP will be considered a covered transaction.

Alan F. Estevez
Questions for Record
Of
Representative Gwen Moore
Subcommittee on Monetary Policy and Trade
Hearing
Evaluating CFIUS: Challenges Posed by a Changing Global Economy

Section 3(a)(5)(B) of the proposed legislation would treat as a covered transaction any transaction involving the contribution by a US critical technology company of intellectual property and associated support. The legislation defines a US critical technology company as any company that produces, trades in, designs, tests, manufactures, services or develops critical technologies. The definition in the proposed legislation of "critical technologies" is very broad and leaves room for further expansion through regulations.

Can each of the witness please answer the following questions: The current CFIUS regulations already define "critical technologies" with specific reference to export controlled regulations? CFIUS has said on page 37 of its most recent annual report that export control regulations "were determined to be the most reliable and accurate means of identifying critical technologies." If that's the case, then there is no apparent reason to change that definition, and it would seem that the best way to deal with the transfer of critical technologies is through the export control regulations, not CFIUS. Don't you agree?

The Export Control Regulations are a reliable guide to identifying critical technologies. However, in todays the rapidly changing technology environment, the Export Control regulation cannot be the only measure as to whether a technology is a critical technology. During my time in the Department of Defense, we consulted with technology experts from the Department's laboratories and experimental units, as well as with our acquisition experts, to determine if the technology involved in a any particular CFIUS case should be considered a critical technology that should not be eligible for transfer to a given nation.

Alan F. Estevez

"Examining the Operations of the Committee on Foreign Investment in the United States"
Monetary Policy and Trade Subcommittee
December 14, 2017
Rep. Andy Barr (R-KY)

Questions for the Record

1. (Mr. Wolf and Mr. Estevez) - Currently, unlike nearly any other such review processes in the U.S. government, parties to a proposed transaction under CFIUS pay no fees for the security review.
   - Does this make sense?
   - Could the entire process be funded through fees?
   - Would fees drive investments to some other country?

   I believe that a fee structure for CFIUS filing does make sense, although I do not believe the entire process could be funded through fees. Any cost structure would need to be analyzed to determine what structure could deter investment. It is important to recognize that CFIUS may impose certain mitigation costs on the transacting parties. However, when that occurs, there is still a government cost to monitoring mitigation agreements.

2. (Mr. Wolf and Mr. Estevez) - Due to the massive increase in volume and complexity of foreign investment, it seems CFIUS has had to devote greater and greater amounts or resources to "knowing what it doesn't know"—trying to find deals that have not been through the CFIUS process, but should. Some proposals for reform suggest a notification to CFIUS of all transactions that might need a review, whether they formally apply for a review or not.
   - Would this increase, or decrease, the CFIUS workload?
   - Would it decrease the chance that companies inadvertently or intentionally went through without a CFIUS review?
   - Should there be some expedited approval based on a notification, or would creating an expedited review process inevitably lead to a dangerous transaction getting waved through in the interest of time?

   I believe that requiring notification of all transactions that might need a review would significantly increase CFIUS workload, but this is probably necessary to protect national security. It would decrease that chance that transactions inadvertently or intentionally went through without a CFIUS review. I do believe that establishing an expedited approval based on notification could work so long as Treasury clearly defines the criteria for such an expedited review. The 30 day review period is currently stressed and the volume would likely increase significantly. Note that CFIUS needs to be adequately resourced across its structure if a volume increase is legislated or regulated, or the process will likely fail to meet objectives of clearing appropriate transactions while protecting national security.

Alan F. Estevez

"Examining the Operations of the Committee on Foreign Investment in the United States"
Monetary Policy and Trade Subcommittee
December 14, 2017
Rep. Andy Barr (R-KY)

Questions for the Record

3. (Mr. Wolf and Mr. Estevez) - Was there ever a time in your tenure when you thought the intelligence community didn't have enough time to complete its own scrub of a proposal, or that the intelligence community expressed concerns about being rushed?

   During my tenure, I always had the intelligence products I needed to make a CFIUS decision, even I asked additional questions or I identified additional data I asked the intelligence community to address. In such cases, the intelligence community was responsive. The Intelligence Community never expressed concerns that they felt rushed to me, although if they did feel rushed, they would likely have expressed that to Treasury.

4. (Mr. Kimmitt, Mr. Estevez, Mr. Wolf, and Ms. McLernon) - Would you explain the concept of "balance" between the need for foreign direct investment and national security, in the context of CFIUS?

   The CFIUS process is designed to protect national security, and as I stated, I believe it did protect critical technologies and critical locations during my tenure. However, I do believe it is important that investors not view the CFIUS process as a roadblock to investing in or doing business in the United States. Foreign investment can drive innovation and create economic vitality – both of which are important to national security. In addition, it is important that the CFIUS process not be viewed as a protectionist trade mechanism that could lead nations to place restrictions on US companies. While national security must be paramount, CFIUS must only prohibit or mitigate cases in which national security is truly at risk.

5. (Mr. Kimmitt, Mr. Estevez, and Mr. Wolf) - Some observers of the current CFIUS statute believe the committee has no jurisdiction over "de novo" or "greenfield" transactions, and others disagree. What is your view?

   I believe that the statute should explicitly allow the CFIUS to review "greenfield" transactions involving critical technology or co-location near sensitive facilities.

Alan F. Estevez

"Examining the Operations of the Committee on Foreign Investment in the United States"
Monetary Policy and Trade Subcommittee
December 14, 2017
Rep. Andy Barr (R-KY)

Questions for the Record

6. (Mr. Kimmitt, Mr. Estevez, and Mr. Wolf) - Some proponents of CFIUS reform think it is necessary because the definition of "covered transaction" – those transactions that might be subject to CFIUS review—is too limited.
   - Is that true?
   - If we were to modernize the CFIUS process, should we retain the notion of "covered transaction" or just assert that any transition might properly apply for or be subjected to a CFIUS review?

   As I testified, I believe that CFIUS should be modernized to ensure that transactions that may threaten national security, such as joint ventures or transactions involving multiple purchases in a given technology sector, may be reviewed. However, I think a "carte blanche" approach in which covered transactions were not defined, either in law or regulation, would not strike the proper balance between national security and fostering beneficial investment.

7. (Mr. Wolf and Mr. Estevez) - Are the types of transactions coming to CFIUS these days so specialized that we might need specialized personnel and perhaps special hiring authority to get the right sort of people with business backgrounds and security clearances on short notice?

   During my tenure, I believe we were able to access the expertise we needed to properly assess transactions, either drawing on resources across the whole of government or by accessing in expertise from the private sector.

Alan F. Estevez

"Examining the Operations of the Committee on Foreign Investment in the United States (CFIUS)"

December 14, 2017

The Subcommittee on Monetary Policy and Trade hearing

Congressman Robert Pittenger (NC-9)

Questions for the Record

To all panelist:

1. Leaving the question of resources to the side, the panelists mentioned that CFIUS is capable of reviewing covered transactions and assessing the national security implications of those transactions. The challenge, however, is that the majority of cross-border transactions are not submitted to the Committee for review and the current definition of what constitutes a "covered transaction" may exclude currently structured investments that are designed to evade CFIUS review. How is the CFIUS process an effective tool to address the impact of cross-border investments in the United States when the majority of those investments are not subject to CFIUS' review or parties choose not to voluntarily file?

   CFIUS does review transactions that parties have not filed, although this is generally the exception. In my view, filing of clearly covered transactions should be mandated. CFIUS must also develop a process to scan for unfiled transactions that CFIUS should review.

Alan F. Estevez

"Examining the Operations of the Committee on Foreign Investment in the United States (CFIUS)"

December 14, 201

The Subcommittee on Monetary Policy and Trade hearing

Congressman Robert Pittenger (NC-9)

Questions for the Record

2. It has been said that the Government maintains a list of "non-notified transactions" – cross-border transactions that have not been submitted to CFIUS. Some suggest that the number of these non-notified transactions is above 9000. How is CFIUS an effective tool when over the course of 5 years the Committee's annual reports indicate that they may have reviewed about 700 transactions, but over 9000 transactions remain unreviewed. Please address the impact of these non-notified transactions on the national security interests of the US (from a military and industry perspective).

I believe CFIUS should mandate the filing of clearly covered transactions. While most unfiled transactions likely do not threaten national security, CFIUS must develop a process for identifying unfiled covered transactions. CFIUS must be adequately resourced to accomplish this task.

Alan F. Estevez

"Examining the Operations of the Committee on Foreign Investment in the United States (CFIUS)"

December 14, 201

The Subcommittee on Monetary Policy and Trade hearing

Congressman Robert Pittenger (NC-9)

Questions for the Record

3. Mr. Wolf, mentioned that the export laws "could and should" be used to determine critical technologies and that the export laws should complement and not be replaced by CFIUS reviews. But the Department of Commerce has, with one or two exceptions, been administering the Export Administration Regulations pursuant to the emergency authorities granted the President under the International Emergency Economic Powers Act (IEEPA) and the National Emergencies Act (NEA). These authorities do not provide substantive underpinnings for the direction or manner in which the Department administers export controls and leaves the management and policy development to Commerce without guidance from Congress. Given this situation, how should Congress address the substantive limitations inherent in the fact that it continues under emergency powers?

I am not an expert in Export Control laws, but would agree Congress should address the limitations of the use of emergency powers.

Alan F. Estevez

"Examining the Operations of the Committee on Foreign Investment in the United States (CFIUS)"

December 14, 201

The Subcommittee on Monetary Policy and Trade hearing

Congressman Robert Pittenger (NC-9)

Questions for the Record

4. How would the proposed legislation usurp export control authority rather than complement it? As written, the proposed legislation by Senator Cornyn (and his cosponsors) and Representative Pittenger (and his cosponsors) identifies the coordinate relationship between CFIUS and the export laws and moves to the fill gaps left by the inadequacies of the export regimes. Please identify the specific sections of the proposed legislation that creates the challenge Mr. Wolf raised during his presentation.

I am not an expert in Export Control authorities. I note that for export controls to work, the parties must be trusted and willing to comply with the law (as most parties are). Export control authorities and CFIUS must be complimentary. CFIUS should not be the tool to manage export controls.

Alan F. Estevez

"Examining the Operations of the Committee on Foreign Investment in the United States (CFIUS)"

December 14, 201

The Subcommittee on Monetary Policy and Trade hearing

Congressman Robert Pittenger (NC-9)

Questions for the Record

5. Several statements by US Government leadership and studies by various think tanks, indicate that the US is rapidly losing its advantage across technologies and is being challenged even in those technologies where it maintains a lead. Prior to the first export reform effort under the Clinton Administration, the US utilized a "deny and delay" strategy for export controls to maintain a strategic advantage. That strategy shifted to a "run faster" concept that rested on the view that the US could develop technologies faster than its economic or military competitors and maintain its tactical advantages. Mr. Estevez noted that that philosophy remains the prevailing view when it is coupled with the tactical excellence of our US military. Has anyone studied the correlation between a change in the underlying strategy for export controls (i.e., "deny and delay" to "run faster") and the gains US economic and military competitors have made? For example, how has the transfer of technologies to the EAR, which may be more freely shared with China or other destinations, affected the US loss of strategic advantage? Given this loss, the theft of intellectual property and a narrow CFIUS review, please explain how our current legislative and regulatory tools protect US national security interests, as well as critical infrastructure issues.

I am not aware of any study to assess the correlation between a change in the underlying strategy for export controls (i.e., "deny and delay" to "run faster") and the gains US economic and military competitors have made. There are many factors that have influenced the narrowing or loss of military technological advantage, to include globalization of technology, the amount of research and development funding spent by the US government, the military focus on wars against terrorist vice great power

competition over the last decade, and the severe impact of sequestration on the defense budget and defense priorities. Theft and transfer of IP certainly play a role as well. With that said, CFIUS is one tool the government has to protect national security. The government must use all the tools, to include export controls, tax and trade policy, to protect its critical technologies. Finally, the United States must be willing to invest in the research and development needed to maintain technological advantage.

Rep. Andy Barr (R-KY)

4. Economic prosperity is an essential element of national security. Foreign direct investment contributes to economic prosperity, and hence national security, by creating millions of high-paying, high-quality American jobs. The balance that must be struck is to promote an openness to this jobs-producing investment while guarding against any harm to national security that might be caused by individual investments.

5. Although an exceptional use of its authority, FINSA could have been applied to some "de novo" or "greenfield" transactions. An example would be acquisition of land to build a new factory adjacent to sensitive U.S. facilities.

6.

• In my experience, the term "covered transaction," both in statute, regulation, and especially practice, gave CFIUS the authority to review those investments that might cause national security concerns.

• Some form of jurisdictional definition – "covered transaction" or otherwise – is important, but it is also important to give CFIUS the authority to adapt to changing circumstances, such as new technologies and investment vehicles.

Congressman Robert Pittenger (NC-9)

1. My experience was that CFIUS and its member agencies were vigilant about acquisitions both notified and not notified. The area of concern was investments short of acquisitions – e.g. venture or other early stage investments – that gave foreign investors potential access to technology even without acquiring the company that owned the technology.

2. If CFIUS kept a list of "non-notified transactions," that suggests that CFIUS was aware of the transactions and could have taken action to bring the transactions into the CFIUS process. Indeed, FINSA would suggest CFIUS had an obligation to review any transaction of which they were aware that could have raised national security concerns.

4. CFIUS, EAR, and ITAR need to act in tandem, though each has its own statutory authority and responsibility. The key is an interagency process involving all relevant actors who decide the appropriate forum, priority, and resolution for issues raised by cross-border investments.

5. I defer to those with more export control experience. But many of the considerations raised in this question are brought to the CFIUS table for discussion, especially by representatives from State, Defense, and Commerce, in those instances where export control issues under review in other fora affect the acquisition-specific facts of the cases before CFIUS.

Nancy McLernon's Responses to Questions for the Record – Rep. Gwen Moore (WI-04)
Nancy McLernon, president and CEO, Organization for International Investment (OFII)

Question One from Rep. Moore: The proposed legislation covers contributions of IP by critical technology companies, but as written, the IP could relate to any kind of IP that the company possesses. Shouldn't we focus specifically on the contribution of IP related to critical technologies, and not other kinds of technology that a US critical technology company happens to possess?

> **Response:** The Committee on Foreign Investment in the United States (CFIUS) reviews cross-border mergers and acquisitions for possible threats to U.S. national security. Considering international companies from longtime U.S. allied countries provide the vast majority of foreign direct investment entering the United States, mainly in industries totally unrelated to national security, it is important that CFIUS maintains a narrow focus on investment activity that raises national security concerns.

Question Two from Rep. Moore: The current CFIUS regulations already define "critical technologies" with specific reference to export controlled regulations. CFIUS has said on page 37 of its most recent annual report that export control regulations "were determined to be the most reliable and accurate means of identifying critical technologies." If that's the case, then there is no apparent reason to change that definition, and it would seem that the best way to deal with the transfer of critical technologies is through the export control regulations, not CFIUS. Don't you agree?

> **Response:** Yes. The Committee on Foreign Investment in the United States (CFIUS) cannot and should not be considered the United States' only tool to address espionage, trade imbalances or broader national security concerns. Export control regulations and other policies also belong in discussions about how to best protect U.S. national security.

Nancy McLernon's Response to Question(s) for the Record – Rep. Andy Barr (KY-06)
Nancy McLernon, president and CEO, Organization for International Investment (OFII)

Question from Rep. Barr: (Mr. Kimmitt, Mr. Estevez, and Ms. McLernon) – Would you explain the concept of "balance" between the need for foreign direct investment and national security, in the context of CFIUS?

Response: The United States is the premier destination for foreign direct investment (FDI). International companies investing in the United States bring tremendous benefits, such as high levels of research and development (R&D), strong participation in the manufacturing workforce and 24 percent higher compensation than the economy-wide average, to name a few. International companies also broaden America's economy and make it more resilient. After all, when an international company invests in the United States, its home country now has a stake in America's success, which is good for the economy and U.S. foreign policy.

However, the United States has seen its share of FDI decline from 37 percent in 2000 to just 25 percent in 2017. As global competition for FDI grows, it is critical that the United States maintains a nonpoliticized system that provides certainty to investors and prevents the transfer of critical technologies to America's adversaries.

The Committee on Foreign Investment in the United States (CFIUS) reviews cross-border mergers and acquisitions for possible threats to U.S. national security. Considering international companies from longtime U.S. allied countries provide the vast majority of FDI entering the United States, mainly in industries totally unrelated to national security, it is important that CFIUS maintains a narrow focus on investment activity that raises national security concerns.

Nancy McLernon's Responses to Questions for the Record – Rep. Robert Pittenger (NC-9)
Nancy McLernon, president and CEO, Organization for International Investment (OFII)

Question One from Rep. Pittenger: Leaving the question of resources to the side, the panelists mentioned that CFIUS is capable of reviewing covered transactions and assessing the national security implications of those transactions. The challenge, however, is that the majority of cross-border transactions are not submitted to the Committee for review and the current definition of what constitutes a "covered transaction" may exclude currently structured investments that are designed to evade CFIUS review. How is the CFIUS process an effective tool to address the impact of cross-border investments in the United States when the majority of those investments are not subject to CFIUS' review or parties choose not to voluntarily file?

> **Response:** Considering international companies from longtime U.S. allied countries provide the vast majority of foreign direct investment (FDI) entering the United States, predominately in industries totally unrelated to national security, it is important that CFIUS maintains a narrow focus on investment activity that raises potential national security concerns.
>
> The bicameral, bipartisan *Foreign Investment Risk Review Modernization Act* (FIRRMA) creates four new types of covered transactions under CFIUS's jurisdiction. FIRRMA also more closely aligns CFIUS reviews with transactions that could lead to the potential transfer of critical technologies.

Question Two from Rep. Pittenger: It has been said that the Government maintains a list of "non-notified transactions" – cross-border transactions that have not been submitted to CFIUS. Some suggest that the number of these non-notified transactions is above 9000. How is CFIUS an effective tool when over the course of 5 years the Committee's annual reports indicate that they may have reviewed about 700 transactions, but over 9000 transactions remain unreviewed. Please address the impact of these non-notified transactions on the national security interests of the US (from a military and industry perspective).

> **Response:** More than 80 percent of FDI activity in the United States takes place through mergers and acquisitions (M&A). Considering international companies from longtime U.S. allied countries provide the vast majority of FDI entering the United States, predominately in industries totally unrelated to national security, it is important that CFIUS maintains a narrow focus on investment activity that raises potential national security concerns.
>
> The United States' open investment climate helps to diversify America's economy and open new markets. International companies in the United States produce 23 percent of U.S. exports, which totals nearly one billion dollars of exports every single day. Moreover, these companies source hundreds of billions of dollars in goods and services from local U.S. suppliers, supplementing their already tremendous contributions to U.S. industry and the U.S. economy.

Question Three from Rep. Pittenger: Mr. Wolf, mentioned that the export laws "could and should" be used to determine critical technologies and that export laws should complement and not be replaced by CFIUS reviews. But the Department of Commerce has, with one or two exceptions, been administering the Export Administration Regulations pursuant to the

emergency authorities granted the President under the International Emergency Economic Powers Act (IEEPA) and the National Emergencies Act (NEA). These authorities do not provide substantive underpinnings for the direction or manner in which the Department administers export controls and leaves the management and policy development to Commerce without guidance from Congress. Given this situation, how should Congress address the substantive limitations inherent in the fact that it continues under emergency powers?

Response: This issue is outside of the scope of OFII's focus.

Question Four from Rep. Pittenger: How would the proposed legislation usurp export control authority rather than complement it? As written, the proposed legislation by Senator Cornyn (and his cosponsors) and Representative Pittenger (and his cosponsors) identifies the coordinate relationship between CFIUS and the export laws and moves to fill the gaps left by the inadequacies of the export regimes. Please identify the specific sections of the proposed legislation that creates the challenge Mr. Wolf raised during his presentation.

Response: Mr. Wolf's testimony stated that "the CFIUS and export control systems complement each other." This approach allows for CFIUS's focus to remain on reviewing FDI transactions for possible national security concerns.

Question Five from Rep. Pittenger: Several statements by US Government leadership and studies by various think tanks, indicate that the US is rapidly losing its advantage across technologies and is being challenged even in those technologies where it maintains a lead. Prior to the first export reform effort under the Clinton Administration, the US utilized a "deny and delay" strategy for export controls to maintain a strategic advantage. That strategy shifted to a "run faster" concept that rested on the view that the US could develop technologies faster than its economic or military competitors and maintain its tactical advantages. Mr. Estevez noted that the philosophy remains the prevailing view when it is coupled with the tactical excellence of our US military. Has anyone studied the correlation between a change in the underlying strategy for export controls (i.e., "deny and delay" to "run faster") and the gains US economic and military competitors have made? For example, how has the transfer of technologies to the EAR, which may be more freely shared with China or other destinations, affected the US loss of strategic advantage? Given this loss, the theft of intellectual property and a narrow CFIUS review, please explain how our current legislative and regulatory tools protect US national security interest, as well as critical infrastructure issues.

Response: The United States is the premier destination for FDI. International companies investing in the United States bring tremendous benefits, such as high levels of research and development (R&D), strong participation in the manufacturing workforce and 24 percent higher compensation than the economy-wide average, to name a few. International companies also broaden America's economy and make it more resilient. After all, when an international company invests in the United States, its home country now has a stake in America's success, which is good for the domestic economy and U.S. foreign policy.

The Committee on Foreign Investment in the United States (CFIUS) cannot – and should not – be construed as the United States' only tool to address espionage, trade imbalances or broader national security concerns. CFIUS's effectiveness lies in its narrow mandate to review cross-border mergers and acquisitions for possible national security concerns. The resulting bipartisan, bicameral legislation struck the proper balance between protecting U.S. national security and establishing a stable, rules-based environment that encourages FDI.

OFII is not aware of any research comparing the effectiveness in approaches on CFIUS.

Responses of Kevin Wolf [in bold] to

Questions for Record
Of
Representative Gwen Moore
Subcommittee on Monetary Policy and Trade
Hearing
Evaluating CFIUS: Challenges Posed by a Changing Global Economy

Section 3(a)(5)(B) of the proposed legislation would treat as a covered transaction any transaction involving the contribution by a US critical technology company of intellectual property and associated support. The legislation defines a US critical technology company as any company that produces, trades in, designs, tests, manufactures, services or develops critical technologies. The definition in the proposed legislation of "critical technologies" is very broad and leaves room for further expansion through regulations.

Can each of the witness please answer the following questions:

> The proposed legislation covers contributions of IP by critical technology companies, but as written, the IP could relate to any kind of IP that the company possesses. Shouldn't we focus specifically on the contribution of IP related to critical technologies, and not other kinds of technology that a US critical technology company happens to possess?
>
> **Response: Yes, absolutely. This question goes right to the heart of what appears to be an inadvertent, but nonetheless significant, over-control in the bill's inbound and outbound investment provisions – paragraphs (5)(B)(iii) and (5)(B)(v). The purpose of the bill with respect to such provisions is to give CFIUS jurisdiction over transactions that would or might result in the contribution of critical technology to foreign persons as a result of an inbound or an outbound investment. The jurisdictional hook of the two paragraphs is, however, not the critical technology that might be contributed or released, but rather the company itself – even if the investment at issue would have nothing to do with critical technology.**
>
> **That is, an inbound investment is caught by paragraph (5)(B)(iii) if it is in a "critical technology company." An outbound investment is caught by paragraph (5)(B)(v) if it is by a "critical technology company." (There are some other requirements and exceptions, but this is the essential jurisdictional hook in the two provisions.) The definition of "critical technology company" is quite broad and includes any company that merely "trades in" or "services" -- not just develops -- an item on one of the export control lists (see (8)(b)(i)-(v)) or in the bill's unidentified list of emerging critical technologies in paragraph (8)(B)(vi). Thus, for example, a company that merely trades in one of the commercial items on the Commerce Control List (such as telecommunications server with commercial encryption), but does not have any ability to develop such technology, is a "critical technology**

company." Any investment into that company (other than a narrowly defined passive investment) would be a covered transaction even if the investment had nothing to do with critical technology or the company had no ability to develop critical technology.

Even for companies that develop critical technology, the jurisdictional scope of paragraphs (5)(B)(iii) and (5)(B)(v) is out of focus because not every investment into or by such companies pertains to, involves, or could result in the contribution of critical technology. An extreme example of this to make the broader point would be a foreign investment in an aerospace company's souvenir coffee cup division. Aerospace companies are critical technology companies, according to the bill's definition of the term, because they develop technologies on the Commerce Control List (among other things). A foreign investment in that company's coffee cup division – which would not result in the contribution of critical technology – would be a covered transaction under (5)(B)(iii) and an outbound joint venture by the coffee cup division with a foreign entity would be a covered transaction under (5)(B)(v). Of course, such investments present no national security threats, but this is an example of how broad the scope provisions are and why the absence of a jurisdictional hook to the critical technology of concern should be addressed to better accomplish the bill's objectives without creating significant inadvertent controls and uncertainties.

The scope of the provisions is even broader when considering that a company could be a "critical technology company" even it never trades in, services, or develops an item on an export control list but engages in such acts with an unknown, unidentified list of emerging technologies in paragraph (8)(B)(vi). There is nothing wrong with the definition of emerging technologies of concern in paragraph (8)(B)(vi). Anything meeting that definition that is not controlled somehow for release to foreign persons should be. I don't think anyone objects to this point, even if they have different ways of articulating the concern. The problem though is that U.S. businesses and foreign investors would have no way of knowing what the government considers to be emerging technology covered by this paragraph because the bill doesn't require the government to identify what types of technologies meet the definition. (The bill does require that regulations be published, but doesn't require a process for the government to identify what the technologies are that meet this definition.)

Thus, U.S. businesses not involved in technology on an export control or other list would not know if they are a "critical technology company" and foreign investors would not know whether they are investing in a "critical technology company." If this were to become law – without a requirement to identify first the emerging technologies of concern -- it could create significant uncertainty in the investment marketplace. U.S. and foreign companies could never really know whether CFIUS would have the authority to unwind or alter a transaction that would involve a company unwittingly trading in, servicing, or developing a technology the government considered to be within the scope of paragraph (8)(B)(vi). Companies

would be discouraged from investing as a result and foreign companies might choose to invest in non-U.S. companies where such uncertainties didn't exist. Again, if the technology is critical and meets the definition in (8)(B)(vi), it should be controlled. No one I know of is objecting to that point. Rather, the issue is the uncertainty about what would meet this definition, particularly for companies that do not work in the national security arena and would not have an intuitive sense for what would be of concern to the government's national security experts.

There are two relatively easy fixes for these issues that would address the national security concerns motivating the bill (which I'm not disagreeing with) but without the inadvertent over-control and uncertainty. One approach would be to first require the government to identify the types of emerging technologies of concern within the scope of paragraph (8)(B)(vi) and then tie the jurisdictional hooks of paragraphs (5)(B)(iii) and (5)(B)(v) to any critical technologies identified in the export control lists or the newly identified technologies within the scope of paragraph (8)(B)(vi). Another approach would be to require the existing technology transfer control system – i.e., the export control system – to identify on the relevant control list (e.g., the Commerce Control List) the technologies that meet the definition in (8)(B)(vi) and then to regulate their transfer to end users, end uses, and destinations of concern under the related export control regulations (e.g., the Export Administration Regulations).

The current CFIUS regulations already define "critical technologies" with specific reference to export controlled regulations. CFIUS has said on page 37 of its most recent annual report that export control regulations "were determined to be the most reliable and accurate means of identifying critical technologies." If that's the case, then there is no apparent reason to change that definition, and it would seem that the best way to deal with the transfer of critical technologies is through the export control regulations, not CFIUS. Don't you agree?

Response: I agree. See my comments above.

Some have argued that export controls cannot address "know-how" or "foundational information." That is not correct. The existing definition of "development" in the Export Administration Regulations includes within its scope all information prior to the production stage necessary to develop an item. 15 C.F.R. 772.1. All that is required is for BIS, working with its interagency colleagues, to identify those early-stage technologies that are of concern and to add them to the controls in the Export Administration Regulations. See 15 C.F.R. Part 774. This is the hard part. Beginning on page 7 of my testimony before HFAC, I describe the existing authorities in the EAR to do so. See: http://docs.house.gov/meetings/FA/FA00/20180314/107997/HHRG-115-FA00-Wstate-WolfK-20180314.pdf

It is also a specific requirement in section 109 of the Export Control Reform Act (H.R. 5040) introduced by Congressmen Royce and Engel. As described at the end

of my HFAC testimony, I believe that this approach would address the concern far more directly and far more quickly – and regardless of whether there were a covered transaction involved. Please do not take this comment as one suggesting that I am hostile to the objectives of FIRRMA. I'm not. Indeed, I think it is in our national security interests that the topics in the bill be addressed. On this one point, however, I believe, based on my experience in the government and in the private sector, that there is already an existing system, the export control system, that can address concerns about technology transfers more directly and with fewer collateral consequences. I make no comment here about other concerns FIRRMA is designed to address.

Kevin Wolf's Responses [in bold] to:

"Examining the Operations of the Committee on Foreign Investment in the United States"
Monetary Policy and Trade Subcommittee
December 14, 2017
Rep. Andy Barr (R-KY)

Questions for the Record

1. (Mr. Wolf and Mr. Estevez) - Currently, unlike nearly any other such review processes in the U.S. government, parties to a proposed transaction under CFIUS pay no fees for the security review.
    - Does this make sense?
    - Could the entire process be funded through fees?
    - Would fees drive investments to some other country?

Response: Yes, to the first question – so long as the Departments that are members of CFIUS properly fund their CFIUS staff to do what needs to be done so that the process is efficient, fair, and responsive to its national security mission. The basis for my "yes" answer is my experience with respect to the prohibition in the Export Administration Act of 1979 against the charging of fees for the filing of export license applications. I believe Congress made a good policy decision with this prohibition because it eliminates the possibility that an agency responsible for a regulatory requirement is even subconsciously affected in its regulatory decisions by a need to generate funds for its operations. The tasks required to address particular national security issues (such as those within the responsibility of CFIUS or the export control system) should be identified. Congress and the responsible agencies should then appropriate and spend the funds to administer the system necessary to perform those tasks – no more and no less. (A corollary belief of mine is that penalties paid for violating the requirements of, for example, the export control rules should go into the general treasury rather than back to the specific law enforcement agency. This helps keep the focus on the substance of the violations rather than how much income they would bring into the enforcing agency.)

No, to the second question. As you know, there is not one appropriation for CFIUS. Each member department decides for itself out of existing funds for the department how to staff its work for the committee. Also, different CFIUS filings require calling upon different parts of the government with expertise that are not normally part of CFIUS. The intelligence community also must reach in to different parts of its system not normally part of CFIUS reviews to collect information that become relevant for different cases. I'm not a budgeting expert, but trying to connect fees to this far-flung

and massive staff efforts in a dozen or so different agencies seems very difficult. I think it is best for each department to have a line-item budget allocation (that doesn't detract from the department's other core missions) for the staff it needs to perform its volume of work required by the pace and difficulty of CFIUS filings. Also, there is a significant sequencing issue in the bill that means that fees cannot pay for all that CFIUS would need to do. That is, the bill's key requirements do not become effective until after there are regulations and staff in place to handle the new workload. (This is a clever timing idea, by the way, that prevents unfunded mandates.) However, to hire the large number of new staff (hundreds?) required to implement the requirements of the new law, there will need to be funds in place a year or more before the effective date to hire, get cleared, and train the new staff to handle the new workload. This is no small task. Thus, a significant source of funds other than fees will be necessary to get the new system started.

Maybe, on the third question. Part of what motivated the bill is a concern about small start-ups and the technology they may develop that is critical. The bill does not want to do anything to discourage U.S. innovation. One percent of a transaction in a low-margin transaction with a small company could be psychologically significant to decisions about whether to invest. I answer "maybe" because I do not have any data or quality anecdotes upon which to base a conclusion. More than the one percent (or $300,000) amount, however, the issue of the fixed costs, expenses, and delays associated with the need to submit a CFIUS filing are significant. It takes a lot of effort to prepare even a short CFIUS filing because of the need to be accurate (so as not to inadvertently make a false or misleading statement to the government) and to collect enough details about a transaction to make the filing complete. There are often follow-on questions from the committee that take time and resources to respond to.

I have seen first hand that the delay involved in getting clearances can result in decisions to avoid transactions. I'm not saying that there should not be CFIUS or export controls, only stating a common point that if they are not administered efficiently and the least regulatory burdensome way possible companies will often choose to avoid the United States for investments in other allied countries with fewer regulatory burdens. There is not data to prove these points because they are events that never happened. I would encourage the members to ask industry for answers to this question to get more reliable, robust answers.

2. (Mr. Wolf and Mr. Estevez) - Due to the massive increase in volume and complexity of foreign investment, it seems CFIUS has had to devote greater and greater amounts or resources to "knowing what it doesn't know"—trying to find deals that have not been through the CFIUS process, but should. Some proposals for reform suggest a notification

to CFIUS of all transactions that might need a review, whether they formally apply for a review or not.

- Would this increase, or decrease, the CFIUS workload?
- Would it decrease the chance that companies inadvertently or intentionally went through without a CFIUS review?
- Should there be some expedited approval based on a notification, or would creating an expedited review process inevitably lead to a dangerous transaction getting waved through in the interest of time?

Response to first bullet: Yes, this would, by definition, increase the workload. By how much is a function of what CFIUS would require be filed. All such discussions always come down to identifying the types of transactions that warrant some form of notification to the government – whether a filing or some form of notice. And to know what to file, the government must first decide what the technology transfers are that present or potentially present some form of a threat that must be regulated. The DIUx study, the 301 report, and other studies (properly) point out issues with a variety of industries, such as Artificial Intelligence, robotics, semiconductors, driverless vehicle technology, and aerospace. To require every transaction or uncontrolled technology transfer in such whole industries to be noticed to the government would be unmanageable – for industry and for the government. Indeed, the sector-wide filing requirements would be significantly harmful to the U.S. industrial base for a wide variety of reasons. (I do not believe that the bill's proponents are advocating whole-sector notice/filing requirements, but I mention to help respond to the question.)

This is where Section 109 of Export Control Reform Act (H.R. 5040) becomes relevant. It would require the Administration to follow an interagency process to identify the emerging technologies of concern and control them. Following this process could result in a more tailored list of technologies that warrant either a full filing or notice requirement – either as part of the regular export control system or a tailored scoping of the outbound and inbound investment provisions of FIRRMA.

With respect to the second bullet, a company could only inadvertently miss a CFIUS process if CFIUS had jurisdiction over the activity. But, assuming a tailored notice requirement could be created, then its success will be a function of how well known it is and if there are sufficient penalties for failing to file (which will motivate more compliance). CFIUS is not well known among the new sectors that would be subject to any new filing requirements, particularly start-ups that generally do not have robust regulatory compliance programs. Thus, a substantial educational and outreach effort would be required to get the word out.

There are three solutions that come to mind (although there would others with more thought). 1. Provide resources for CFIUS to hire staff to travel the country to educate those who would be affected. 2. Provide resources to BIS for its already existing exporter services staff to get the word out. (The work would dovetail with its export control education responsibilities.) 3. Think of a clever way to connect the

obligation to the patent application process. Although many of the newly affect companies may not have robust regulatory compliance systems, they will want to apply for and protect their patents. The U.S. government already (to some extent) reviews patent filings for national security issues. Combining the new CFIUS notice obligation with existing national security patent review process might be efficient.

With respect to the third question, again, the key is how broad or narrow the scope of the filing requirement is. There is always a risk that artificially expedited procedures will result in review failures. The key is to have a process to (i) identify the national security threats for which technologies, (ii) tailor the requirements to that threat, (iii) educate the public on the new requirements after a notice and comment process to work out errors, (iv) assess how many staff will be required to review and process the new filings in a reasonable time, such as thirty day.

3. (Mr. Wolf and Mr. Estevez) - Was there ever a time in your tenure when you thought the intelligence community didn't have enough time to complete its own scrub of a proposal, or that the intelligence community expressed concerns about being rushed?

   Response: No. If further investigation was required, we sent the cases into investigation. If that was not enough to resolve issue, we often informally asked parties to withdraw and re-file the submission so that we could continue the work.

4. (Mr. Kimmitt, Mr. Estevez, Mr. Wolf, and Ms. McLernon) - Would you explain the concept of "balance" between the need for foreign direct investment and national security, in the context of CFIUS?

   Response: National security concerns are, of course, paramount and should be the basis for any final CFIUS actions. The United States never wants to be in a fair fight. The appropriate, aggressively enforced, clearly written, and *well-funded* foreign direct investment, export, and related controls are a critical part of maintaining that advantage. I have never subscribed to the view that CFIUS requirements or export controls should "balance" national security concerns with economic concerns. National security concerns are not to be traded off for something else in a particular transaction or in trade deals. Rather, they should be properly calibrated, tailored controls to avoid collateral economic costs, unnecessary regulatory burdens, and misallocation of federal resources. If controls are too broad – e.g., applicable to entire sectors of an economy rather than particular transactions or technologies – the U.S. industrial base is harmed because investment in benign aspects of the sector gravitates toward similar investments in allied countries without such controls. If the scope is too narrow, then, of course,

the national security is harmed as well because the objectives of CFIUS – resolving national security risks associated with foreign investment are not addressed. As importantly, their scope must be certain so that companies (foreign and domestic) can easily know when they apply. Otherwise, the uncertainty creates incentives to avoid transactions with U.S. companies, which inevitably hurts the US industrial base.

I realize this answer is quite general. If you'd like a longer commentary, let me know. If it is a difficult question to address briefly.

5. (Mr. Kimmitt, Mr. Estevez, and Mr. Wolf) - Some observers of the current CFIUS statute believe the committee has no jurisdiction over "de novo" or "greenfield" transactions, and others disagree. What is your view?

   Response: It is not an opinion – Under current law and regulations, CFIUS does not have jurisdiction over foreign investments that are not "covered," i.e., do not or would not result in control, as defined, of a U.S. business. Thus, if there is no U.S. business that would be subject to control, then CFIUS doesn't have jurisdiction. (Counsel can provide a more detailed answer with citations, but this is the essential point.)

6. (Mr. Kimmitt, Mr. Estevez, and Mr. Wolf) - Some proponents of CFIUS reform think it is necessary because the definition of "covered transaction" – those transactions that might be subject to CFIUS review—is too limited.
   - Is that true?
   - If we were to modernize the CFIUS process, should we retain the notion of "covered transaction" or just assert that any transition might properly apply for or be subjected to a CFIUS review?

   Response: Yes. I think the proposed expansion to cover certain types of real estate transactions is a good idea. Expanding the scope to cover additional types of inbound and outbound transactions warrants additional discussion regarding the goals to be achieved. If the purpose of the expansion is to address technology transfer concerns, then the export control system is a better place to address such concerns. It literally exists to identify and regulate the transfers of technology – regardless of the underlying transaction – that warrant control for national security or foreign policy reasons. I applaud FIRRMA's provisions that would make such hiring quicker and easier for the CFIUS agencies.

Retaining the notion of "covered transaction" is clearly the better approach. It allows (with properly drafted regulations) for certainty as to which types of transactions would and would not be subject to the jurisdiction of CFIUS. Without it, massive uncertainty would result about the circumstances under which CFIUS could exert its authority to block or alter a transaction. Such an open-ended authority would significantly harm the US industrial base because it would discourage investment with U.S. companies. When given an option between the possibility of a transaction being unwound in a non-reviewable proceeding that can be imposed without knowledge of when jurisdiction would be applied versus largely unrelated transactions in allied countries, foreign investors will generally prefer the latter. Uncertainty discourages investment.

Moreover, such an open-ended filing requirement is effectively the beginning of an U.S. industrial policy. History has shown that state-controlled alteration of economic decisions eventually harm the economy more than it helps. All previous administrations in recent history have eschewed such tactics. The experience of other countries that try it to a significant scale prove that it distorts economic incentives and reduces profit. Such systems are also prone to political capture where the system is manipulated for individual, market-distorting gain by those in charge. (I'm not an economist, so I will defer to actual economists for a better, more robust description of why industrial policies are, in the main, bad for the economy.)

7. (Mr. Wolf and Mr. Estevez) - Are the types of transactions coming to CFIUS these days so specialized that we might need specialized personnel and perhaps special hiring authority to get the right sort of people with business backgrounds and security clearances on short notice?

Response: In some cases, yes. There is significant expertise within the government in most of the technology topics that come before CFIUS. Also, CFIUS has the authority and the tradition of bringing in subject matter experts from agencies not normally part of the CFIUS process. However, to address the emerging technology issues at the heart of what is motivating FIRRMA, I'd suggest Commerce, Defense, Treasury, and DHS, in particular, look to hiring for their CFIUS review staffs additional non-traditional subject matter experts in the specific emerging technologies under discussion. The government is good at what it knows, but the topic at issue is about what it does not know – and from a purely commercial sector that traditional national security experts in the government may not be as well versed in. I'm not suggesting in any way that current staff are unqualified, only

that they are understaffed – and when hiring new staff, technical experts in the areas under discussion should be the focus.

Kevin Wolf's responses [in bold] to:

Thursday, December 14, 2017

"Examining the Operations of the Committee on Foreign Investment in the United States (CFIUS)"

The Subcommittee on Monetary Policy and Trade hearing

Congressman Robert Pittenger (NC-9)

To all panelist:

1. Leaving the question of resources to the side, the panelists mentioned that CFIUS is capable of reviewing covered transactions and assessing the national security implications of those transactions. The challenge, however, is that the majority of cross-border transactions are not submitted to the Committee for review and the current definition of what constitutes a "covered transaction" may exclude currently structured investments that are designed to evade CFIUS review. How is the CFIUS process an effective tool to address the impact of cross-border investments in the United States when the majority of those investments are not subject to CFIUS' review or parties choose not to voluntarily file?

Response: CFIUS has jurisdiction over foreign investments that would or could result in control of a U.S. business – whether directly or indirectly, formally or informally. Transactions that do not or could not result in control, as broadly defined, of a U.S. business are not covered. That doesn't mean that parties to non-covered transactions were necessarily evading a CFIUS obligation. There are many economic reasons why transactions are structured that are completely unrelated to the concerns CFIUS is designed to address. Thus, the real question is what national security concerns related to foreign investment are not being addressed by other areas of law that could be addressed by expanding the scope of covered transactions to those that would not involve control by a foreign person over a U.S. business. FIRRMA sets out several suggested fixes for several gaps, such as those pertaining to real estate transactions near sensitive military facilities.

The topic I was asked to speak about pertains to whether, as a result of transactions that do not result in control over a U.S. business, there is an unaddressed risk of emerging critical technologies of concern being transferred to foreign persons, primarily those in China. I am not denying that the Chinese government has announced a plan to acquire from the United States a list of essentially commercial technologies that are not subject to current export controls for strategic and military gain. In my role as Assistant Secretary, I

required the creation of new or revised controls to address such concerns and instructed that many licenses be denied based on concerns that otherwise commercial technology might be diverted to a military end use or end user in China and other countries. I continue to be concerned about such issues and am grateful that the FIRRMA discussion has kick-started the debate about how to address such evolving concerns, and how to address them quickly. My essential point in response is that any emerging technologies that meet the standards in FIRRMA section 3(a)(8)(B)(vi) should be identified and controlled -- regardless of the underlying transaction. In testimony I later gave to the House Foreign Affairs Committee, I described these authorities and options in some detail. I'd ask that it be reviewed as part of my answer to this question. See: http://docs.house.gov/meetings/FA/FA00/20180314/107997/HHRG-115-FA00-Wstate-WolfK-20180314.pdf

2. It has been said that the Government maintains a list of "non-notified transactions" – cross-border transactions that have not been submitted to CFIUS. Some suggest that the number of these non-notified transactions is above 9000. How is CFIUS an effective tool when over the course of 5 years the Committee's annual reports indicate that they may have reviewed about 700 transactions, but over 9000 transactions remain unreviewed. Please address the impact of these non-notified transactions on the national security interests of the US (from a military and industry perspective).

Response: From my time in government, I am aware that there were non-notified transactions that CFIUS determined should be reviewed and ordered the parties to file, which they did. I am unaware, however, of a list of non-filed covered transactions that is that large. If it exists, the committee should absolutely review it to determine whether the already-completed transactions should be unwound or altered to address national security concerns. If it does not have the staff to do so, then the departments, working with Congress, should get the appropriations and funding for more staff to review the cases. (The system could barely handle 240 cases last year, so reviewing 9000, or a fraction thereof, more would require a substantially larger CFIUS staff at multiple agencies.)

The broader point to the question is that the process is voluntary under current law and, except for foreign-government controlled transactions, would be under FIRRMA as well. Companies make, and would still need to make, their own determinations about whether a transaction is covered and then about whether it potentially raises any national security implications that might result in CFIUS's later deciding to unwind or alter it. If there were that many transactions covered by the current law that were not filed with CFIUS, then there is not a clear weakness in the current CFIUS definition of covered transaction, only in (a) the ability of companies to realize that there might be a national security concern for the U.S. government with respect to the transaction and (b) the absence of fear that the U.S. government would demand a filing for a non-notified and completed transaction. With respect to the first point, it was not uncommon that national security concerns expressed by the committee to parties came as an apparent surprise to them. Commercial

companies not normally involved in national security applications for their products often do not know how their technology could be put to other uses of concern. This is why it is critical for the U.S. government to identify, even if generally, the types of transactions that would raise national security concerns and then to educate the public about them. The FIRRMA debate is educating the public on such issues and Treasury does some outreach. My suggestion though would be for the government to increase the pace and quantity of outreach in to the issues CFIUS is concerned about, particularly in parts of the country where significant amounts of emerging technologies are being developed. With respect the second point, I and most other witnesses testified that the agencies need more resources to research transactions that were not notified. This would lead to more non-notified filings orders, which would then lead to more companies fearing the economic harm that could result if they did not file a covered transaction that was later determined to have unresolved national security issues.

3. Mr. Wolf, mentioned that the export laws "could and should" be used to determine critical technologies and that the export laws should complement and not be replaced by CFIUS reviews. But the Department of Commerce has, with one or two exceptions, been administering the Export Administration Regulations pursuant to the emergency authorities granted the President under the International Emergency Economic Powers Act (IEEPA) and the National Emergencies Act (NEA). These authorities do not provide substantive underpinnings for the direction or manner in which the Department administers export controls and leaves the management and policy development to Commerce without guidance from Congress. Given this situation, how should Congress address the substantive limitations inherent in the fact that it continues under emergency powers?

Response: I agree with the premise of the question, which is why I support passage (after some technical corrections of inadvertent drafting errors) of the bipartisan Export Control Reform Act of 2018 (H.R. 5040) introduced by Congressmen Royce and Engel. Section 102 of the bill sets out a modern statement of policy for the export control system. It would express the will of Congress regarding what the export control system should achieve. I suspect most members of Congress, Democratic and Republican, would agree with it.

In addition, section 109 of the bill would require the Administration to conduct a "regular, ongoing interagency process to identify emerging critical technologies that are not identified in any list of items controlled for export under United States law or regulations, but that nonetheless could be essential for maintaining or increasing the technological advantage of the United States over countries that pose a significant threat to the national security of the United States with respect to national defense, intelligence, or other areas of national security, or gaining an advantage over such countries in areas where such an advantage may not currently exist." The section goes on to require such technologies be

controlled, unilaterally at first and then multilaterally to keep the playing field for US companies as level as possible with its allies. Although Commerce has the authority to do such work now under IEEPA, such a congressional instruction would motivate the Administration to do more than is done now (or previously) about identifying and controlling such emerging technologies, which are literally the types of uncontrolled technologies at the heart of the FIRRMA concerns.

4. How would the proposed legislation usurp export control authority rather than complement it? As written, the proposed legislation by Senator Cornyn (and his cosponsors) and Representative Pittenger (and his cosponsors) identifies the coordinate relationship between CFIUS and the export laws and moves to the fill gaps left by the inadequacies of the export regimes. Please identify the specific sections of the proposed legislation that creates the challenge Mr. Wolf raised during his presentation.

Response: "Usurp" is perhaps too strong of a word and not something I would have said. My main point on this topic is that there exists already an entire system to identify and regulate the transfer of technology of concern for national security or foreign policy reasons – the export control system. It has several advantages over the some of the investment provisions in FIRRMA. It creates certainty for both US and foreign parties in that it identifies, even if in broad terms, the types of technologies (either in the earliest developmental stages or later production stages) that are and are not controlled. (Uncertainty discourages investment and is thus contrary to the goal of maintaining a healthy industrial base.) The export control system also creates fewer collateral consequences because it is infinitely tailorable to address transfers to specific destinations, end uses, and end users.

Most importantly, export controls regulate technology of concern *regardless of the nature of the underlying transaction.* That is, if technology is sensitive, the export control system requires authorization for its release regardless of whether it would be transferred as part of a joint venture, inbound investment, a telephone call, an email, or a regular response to a purchase order. The FIRRMA approach would only control the technology of concern if there were a covered transaction, however defined. If technology is of such concern that it would warrant the potential unwinding of an investment, then it is of such concern to be regulated generally, with or without an investment. My testimony to HFAC goes into more detail on the scope and flexibility of the export control system. See: http://docs.house.gov/meetings/FA/FA00/20180314/107997/HHRG-115-FA00-Wstate-WolfK-20180314.pdf

As also stated in my HFAC testimony, export controls are not the solution to all problems. If the national security issue associated with an investment does not pertain to technology transfer concerns or imposing prohibitions on specific end users or end uses outside the United States, then the export control system is not the solution.

○